BYOD Wireless Infrastructure Design

Revised: August 7, 2013

The Cisco Wireless LAN Controller (WLC) is used to automate wireless configuration and management functions and to provide visibility and control of the wireless networks. The WLC is able to interact with the Identity Service Engine to enforce authentication and authorization policies across endpoints.

While designing WLAN networks, the following should be considered:

- The role of the WLAN
- The authentication mechanism for the WLAN
- The number of WLANs present in a network

This design guide logically separates the WLAN into distinct logical functions: device provisioning and secure network access. These two functions can be provided by two different WLANs or combined into a single WLAN. This design guide covers both single and dual SSID deployment models for both the branch and the campus locations. Note that in this design guide wireless guest access is implemented on a different WLAN.

Some considerations when selecting a single versus dual SSID configuration:

- Some organizations prefer having a dedicated SSID for on-boarding devices.
- Others see dual SSID as an extra management burden.
- A second SSID adds channel overhead.
- Enabling too many SSIDs may degrade wireless performance.

The organization's unique requirements and preferences will dictate which model to deploy. The configurations of both the ISE and WLC may be easily modified to support either single or dual SSID deployments.

Campus—Unified Wireless LAN Design

As mentioned in Centralized (Local Mode) Wireless Design in Chapter 5, "Campus and Branch Network Design for BYOD," the two wireless LAN designs for the campus which are discussed within this design guide are Centralized (Local Mode) and Converged Access designs. Clients connecting from the campus wireless infrastructure are served by a dedicated cluster of CT5508 Unified Controllers configured in local mode (central switching) or served by a combination of Catalyst 3850 series switches which provide the Mobility Agent (MA) function, while CT5760 wireless controllers provide the Mobility

Controller function. This section discusses the Unified Wireless LAN Design, while discussion on Converged Access follows. The wireless controllers are configured with the proper SSIDs to provide device on-boarding and secure access. This functionality may be provided via single or dual SSIDs.

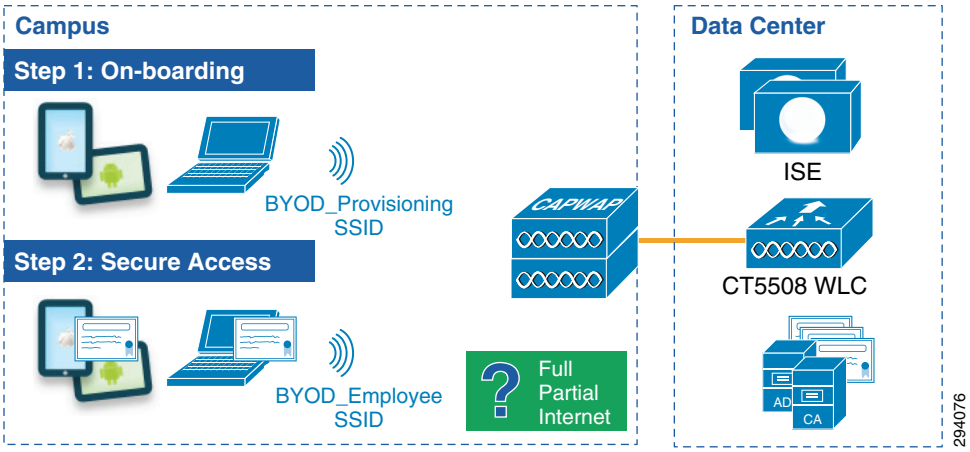
Note The CT5760 wireless controller can also be configured to function as a centralized (Local Mode) wireless controller. As discussed in Campus Migration Path of Chapter 5, "Campus and Branch Network Design for BYOD," this may be a necessary step in migrating from an existing wireless overlay design to a converged access design.

Centralized Campus—Dual SSID Design

In this design there are two SSIDs: one provides enrollment/provisioning and the other provides secure network access. After connecting to the BYOD_Provisioning SSID and completing the enrollment and provisioning steps, the user connects to the BYOD_Employee SSID, which provides network access over a secure EAP-TLS connection.

Figure 9-1 shows the dual SSID design for the campus APs.

Figure 9-1 Campus-Dual SSIDs



In a dual SSID design, there are some additional considerations:

- The provisioning SSID can be either open or password protected. When the provisioning SSID is open, any user can connect to the SSID, whereas if it is password protected, then only users that have credentials, such as AD group membership, are allowed to connect to the SSID. In this design guide, the provisioning SSID is configured to be open and its only purpose is to provide on-boarding services.
- After the device is provisioned, it is assumed that the user will switch to the second SSID for regular network access. To prevent the user from staying connected to the provisioning SSID, an access list that provides only access to ISE, DHCP, and DNS must be enforced on the provisioning SSID. The details of the ACL_Provisioning_Redirect ACL are shown below.
- This design guide makes use of the following SSIDs: BYOD_Provisioning and BYOD_Employee.

The properties of these two SSIDs are highlighted in Table 9-1.

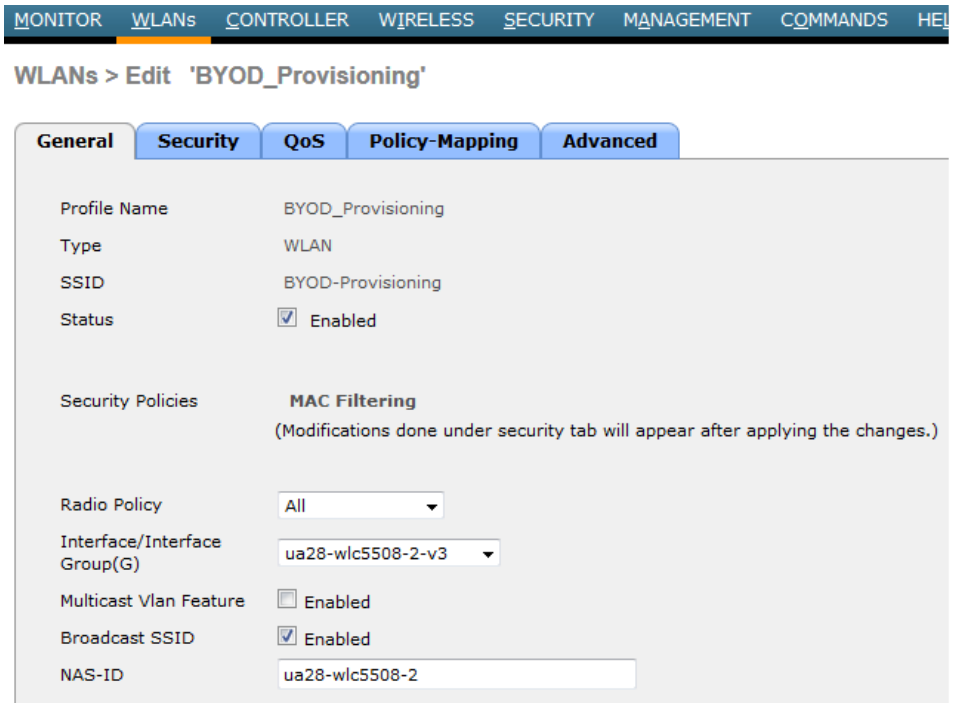
Table 9-1 WLAN Parameters

Attribute	BYOD_Provisioning	BYOD_Employee
Description	Used only for device provisioning	For employees that have completed the on-boarding process
Layer 2 Security	None (for Open SSID)	WPA+WPA2
MAC Filtering	Enabled (for Open SSID)	Disabled
WPA+WPA2 Parameters	None	WPA2 Policy, AES, 802.1X
Layer 3 Security	None	None
AAA Server	Select ISE	Select ISE
Advanced	AAA Override Enabled	AAA Override Enabled
Advanced	NAC State-RADIUS NAC	NAC State-RADIUS NAC
Quality of Service	Best Effort	Platinum
AVC	None	Enabled

To create a WLAN, click **WLANs > Create New > Go** and provide the SSID and profile details. Starting with Figure 9-2 the general configuration steps of the BYOD_Provisioning SSID are highlighted. The steps to configure the BYOD_Employee WLAN are similar, following the settings in Table 9-1.

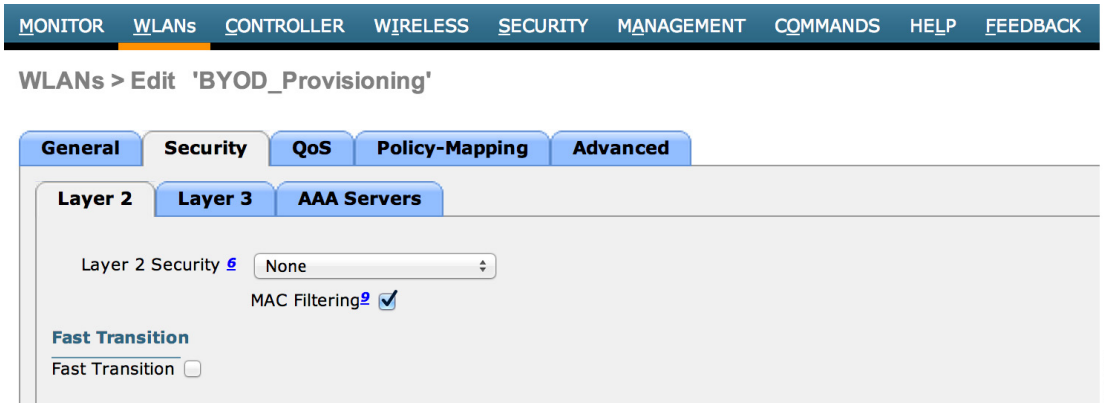
Note When implementing BYOD solutions using more than one Wireless LAN Controller, WLAN IDs must be kept consistent. WLAN ID is used by ISE in determining which WLAN (SSID) clients are using to connect to the network. Ensuring each WLAN has the same WLAN ID on each WLC is essential for proper operation and security.

Figure 9-2 Creating the BYOD_Provisioning SSID



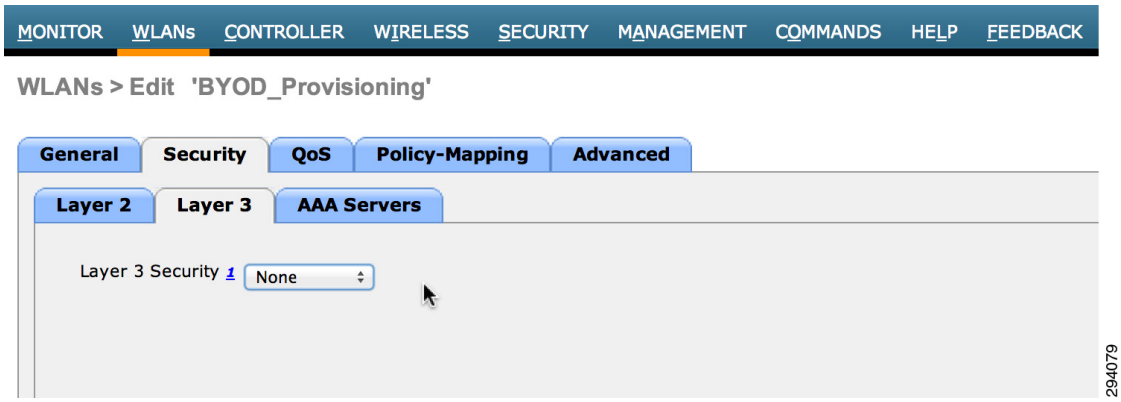
The Layer 2 security settings are configured as **None** since BYOD_PROVISIONING is an open SSID. If the provisioning SSID has to be password-protected, then the Layer 2 security settings must be configured as WPA+WPA2 Enterprise.

Figure 9-3 Layer 2 Security Settings



The Layer 3 Security is configured as **None**, as shown in Figure 9-4.

Figure 9-4 Layer 3 Security Settings



The main configuration in the security settings is to specify the RADIUS server configuration details. Figure 9-5 shows how the ISE's IP address is configured for Authentication and Authorization.

Figure 9-5 AAA Security Settings

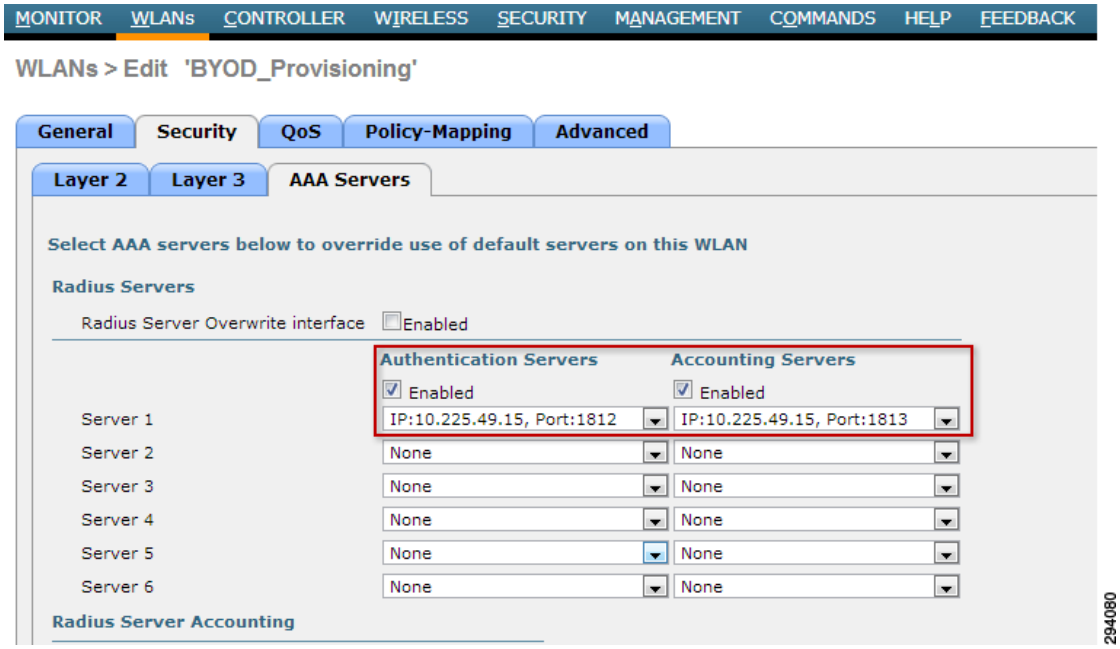
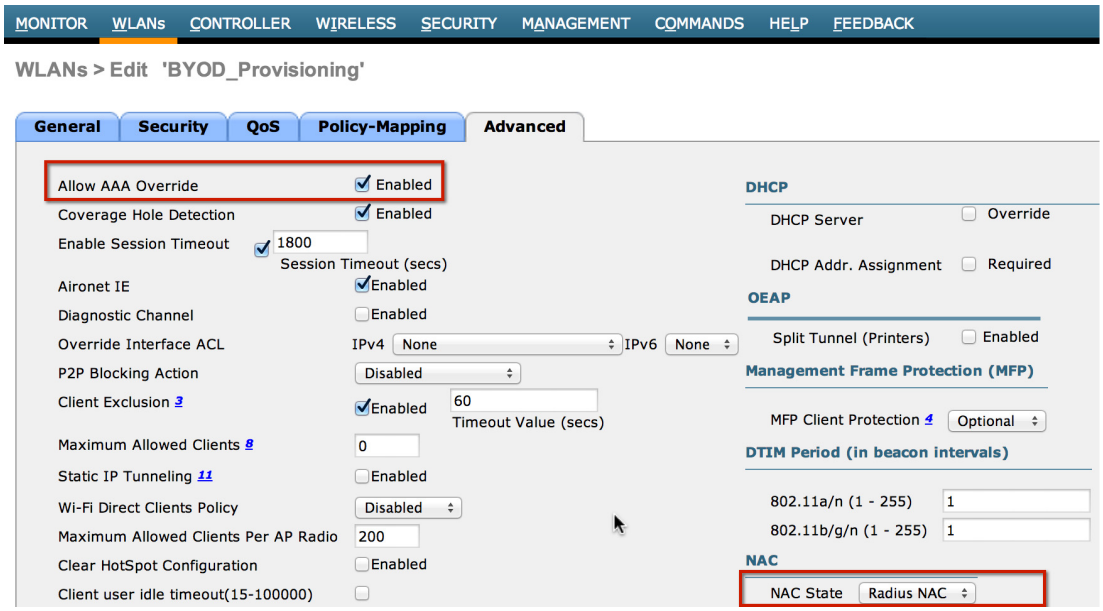


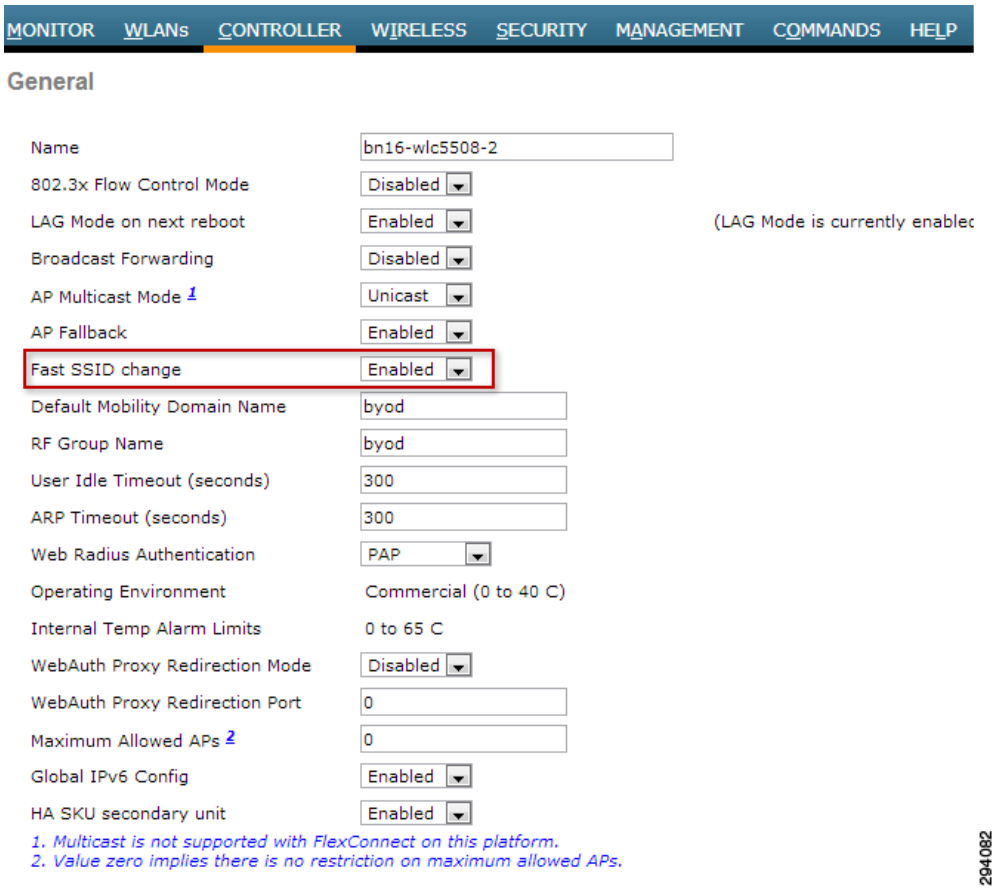
Figure 9-6 shows the advanced settings, including AAA Override and NAC State.

Figure 9-6 Advanced Settings



The Fast SSID Change feature is useful when a device needs to switch from one SSID to another. This applies to the dual SSID BYOD design. After the user completes registration with BYOD_Provisioning, the user is switched to BYOD_Employee SSID. By enabling the FAST SSID Change feature, the user switches immediately to the new SSID without experiencing delays. To enable Fast SSID Change, click **Controller > General > Fast SSID change**, as shown in Figure 9-7.

Figure 9-7 Fast SSID Change

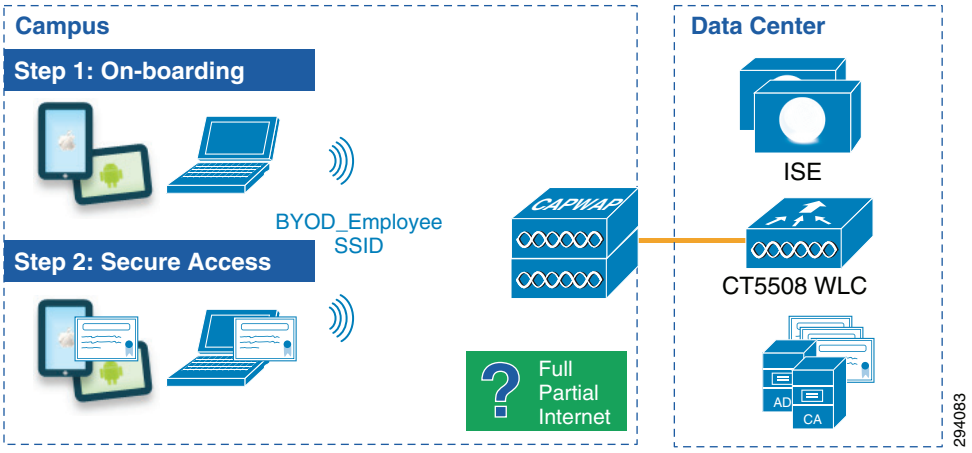


Note Authorization Policies and Profiles in Chapter 10, "Identity Services Engine for BYOD" shows the ACLs and authorization profiles used for dual and single SSID provisioning.

Centralized Campus—Single SSID Design

In a single SSID design the same WLAN (BYOD_Employee) is used for on-boarding and secure network access. Figure 9-8 shows how this design may be implemented using the 5508 Wireless LAN Controller. In this case, the controllers are dedicated to manage the APs in the campus.

Figure 9-8 Campus—Single SSID



Note Authorization Policies and Profiles in Chapter 10, "Identity Services Engine for BYOD" shows the ACLs and authorization profiles used for dual and single SSID provisioning.

Centralized Campus—Policy Enforcement using TrustSec

As discussed in ACL Complexity and Considerations in Chapter 5, "Campus and Branch Network Design for BYOD," past versions of the CVD utilized Named ACLs pre-configured on the wireless controllers to enforce role-based policies for access to network and Data Center resources. This CVD introduces a complimentary technology known as TrustSec and, more specifically, Security Group Access (SGA) to enforce role-based policies through the use of Security Group Tags (SGT) to control access to data center resources. This CVD discusses an approach to slowly migrate to the use of SGT as opposed to, or even in addition to, the use of ACLs through Network Device definitions created in ISE.

Branch—Unified Wireless LAN Design

FlexConnect Wireless LAN Design

In this design guide, endpoints connecting from branch locations are managed by a cluster of Flex 7500 Wireless LAN Controllers or Virtual Wireless LAN Controllers (vWLCs). The vWLC is software which can run on industry standard virtualization infrastructure and is more suitable for small- and medium-sized businesses.

The configuration parameters described in this section apply to both the vWLC and Flex 7500 controllers.

The following link provides more information on how to set up vWLCs using VMware: http://www.cisco.com/en/US/customer/products/ps12723/products_tech_note09186a0080bd2d04.shtml.

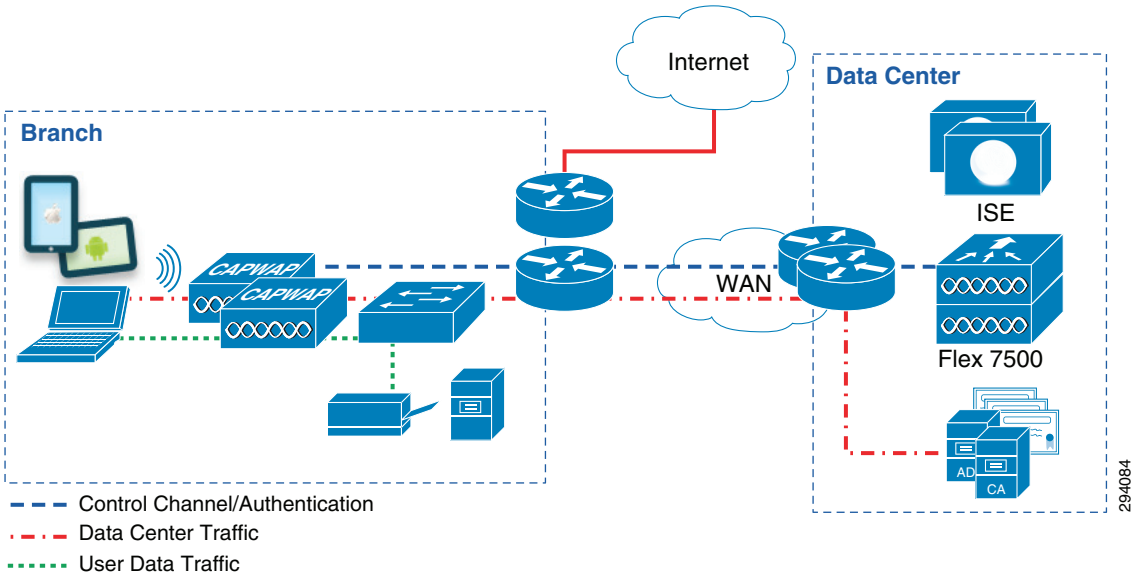
FlexConnect (previously known as Hybrid Remote Edge Access Point or H-REAP) is a wireless solution for branch office and remote office deployments. It enables customers to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost.

Distributing client data traffic using the FlexConnect architecture offers some advantages:

- A controller is not required at each branch location.
- Mobility resiliency within branch during WAN link failures.
- Central management and troubleshooting.

The FlexConnect architecture in Figure 9-9 shows different traffic flows originating at the branch.

Figure 9-9 FlexConnect Architecture



When an endpoint associates to a FlexConnect access point, the access point sends all authentication messages to the controller and either switches the data packets locally (locally switched) or sends them to the controller (centrally switched), depending on the WLAN configuration.

With respect to data packet flows, the WLAN can be in any one of the following modes:

- Central switching—Central switched WLANs tunnel both the wireless user traffic and all control traffic to the centralized WLC, where the user traffic is mapped to a dynamic interface or VLAN.
- Local switching—In this mode the FlexConnect access point switches data packets locally by dropping all traffic locally at the wired interface. Wireless user traffic is mapped to discrete VLANs via 802.1Q trunking.

The Flex 7500 Wireless Branch Controller Deployment Guide offers more details: http://www.cisco.com/en/US/products/ps11635/products_tech_note09186a0080b7f141.shtml.

The key strategy for providing differentiated access to users is done by assigning users to different VLANs dynamically. The AAA Override feature for FlexConnect assigns individual clients to specific VLANs, based on the returned RADIUS attributes from the ISE.

The access point must be preconfigured with all of the possible VLANs that can be returned by the ISE server. The VLAN assignment returned by the ISE as part of authorization is applied. If the VLAN that was returned from the ISE is not present on the AP, the client falls back to the default VLAN configured for the WLAN.

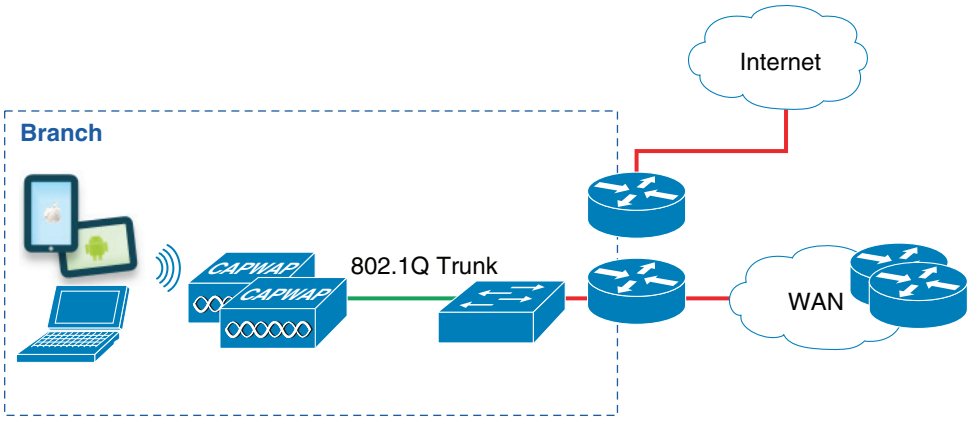
In this design three VLANs have been configured for wireless connectivity on the BYOD_Employee SSID. Table 9-2 illustrates those VLANs and their purpose.

Table 9-2 VLANs and Purpose

VLAN Number	VLAN Name	Description
10	Wireless_Full	Users assigned to this VLAN get full access to campus and branch servers.
11	Wireless_Partial	In addition to Internet access, users assigned to this VLAN access to additional campus and branch resources.
12	Wireless_Internet	Users assigned to this VLAN get only Internet access.
18	AP_Mgmt_Flex	This is the native VLAN that the user will initially be placed into, until the authorization policy determines the appropriate VLAN.

Since more than one VLAN is configured for local switching, FlexConnect APs at the branch must be connected to an 802.1Q trunk link. Both the AP and the upstream switchport need to be configured for 802.1Q trunking. Figure 9-10 shows an example configuration of the access layer switch that connects to the FlexConnect AP.

Figure 9-10 Trunk Configuration



Branch Wireless IP Address Design

Once the device has been dynamically assigned to a VLAN, the endpoint must obtain an IP address from a DHCP server. In the following example the branch router's Layer 3 subinterfaces are configured with the **ip-helper address** command, pointing to a DHCP server:

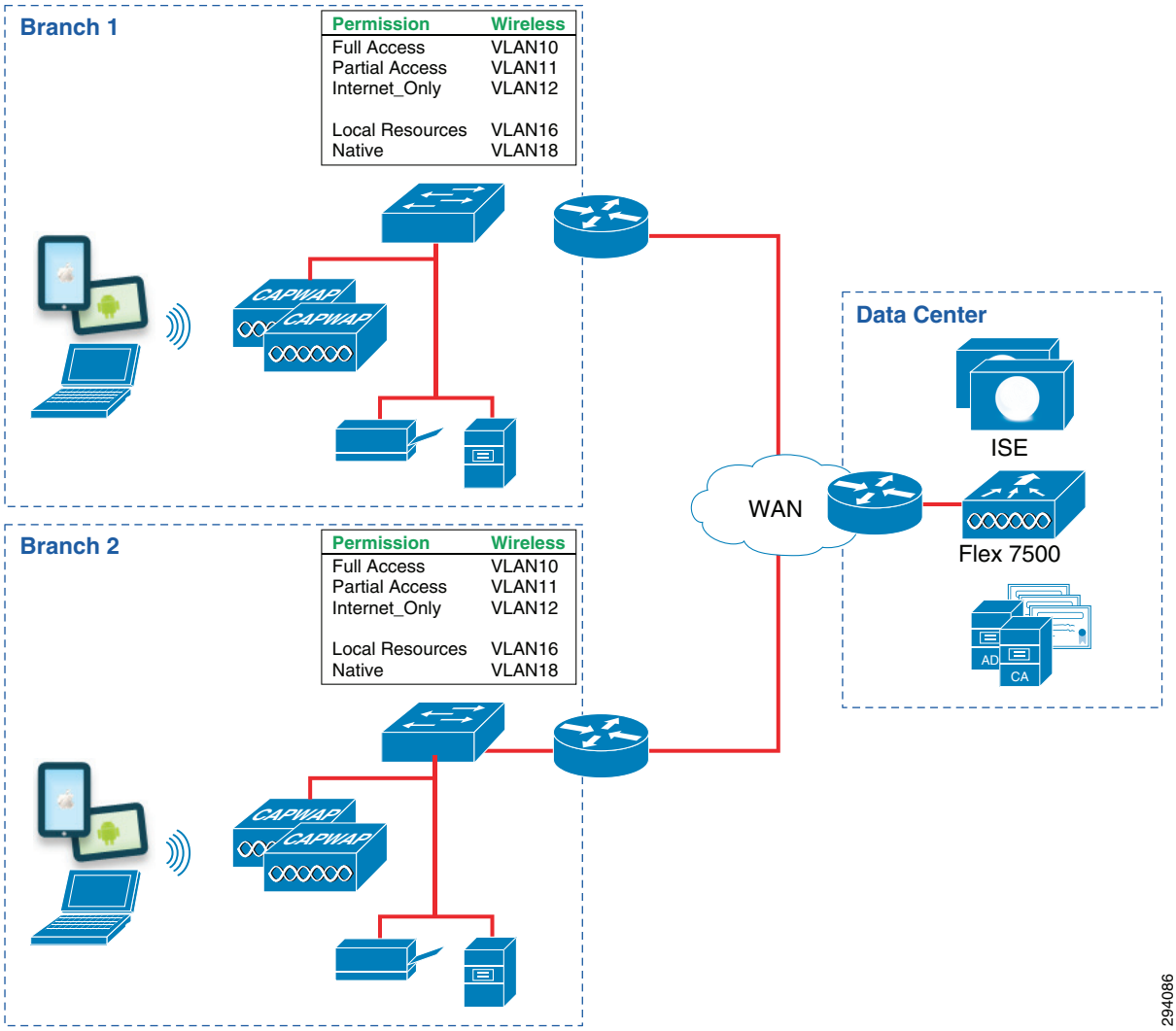
```
interface GigabitEthernet0/1
 description Trunk to branch bn22-3750x-1
 no ip address
 media-type sfp
!
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 10.200.10.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 10 ip 10.200.10.1
 standby 10 priority 110
 standby 10 preempt
!
interface GigabitEthernet0/1.11
 encapsulation dot1Q 11
 ip address 10.200.11.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 11 ip 10.200.11.1
 standby 11 priority 110
 standby 11 preempt
!
interface GigabitEthernet0/1.12
 encapsulation dot1Q 12
 ip address 10.200.12.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 12 ip 10.200.12.1
 standby 12 priority 110
 standby 12 preempt
```

The diagram in Figure 9-11 shows two branch locations utilizing resources from the data center and illustrates the following key points:

- At the branch, endpoints are placed in different VLANs based on the level of access to which they are entitled.
- The wireless infrastructure from the branches is managed by a single cluster of Flex 7500 controllers.
- Endpoints that get assigned to VLAN 10 are granted full access to network resources, VLAN 11 for partial access and VLAN 12 for Internet access.

Based on the matching authorization profile, a user is assigned to a specific VLAN where predefined permissions have been defined.

Figure 9-11 VLANs Used at the Branches

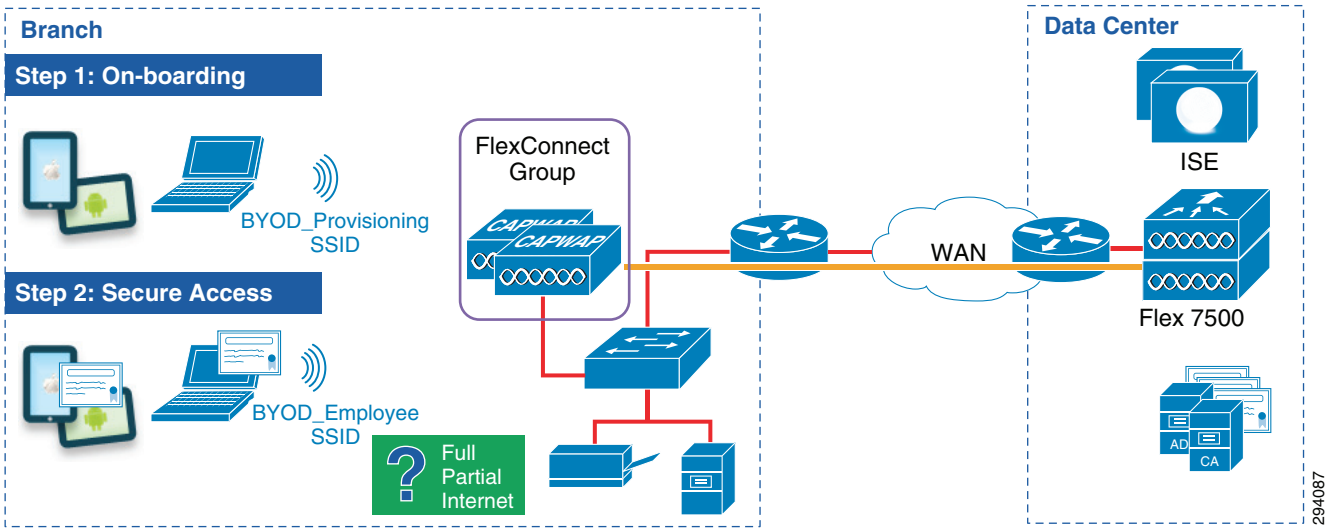


FlexConnect Branch—Dual SSID Design

In the Dual SSID design two SSIDs are configured: one SSID provides enrollment/provisioning while the other provides secure EAP-TLS access. After connecting to the BYOD_Provisioning SSID and completing the enrollment and provisioning steps, the user connects to the BYOD_Employee SSID, which provides secure network access.

Figure 9-12 shows the dual SSID design for the branch APs.

Figure 9-12 Branch-Dual SSIDs



In a dual SSID design, there are some additional considerations:

- The provisioning SSID can be either open or password-protected. When the provisioning SSID is open, any user can connect to the SSID, whereas if it is password protected, then only users that have credentials, such as AD group membership, are allowed to connect to the SSID.
- After the device is provisioned, the user connects via EAP-TLS to the BYOD_Employee SSID for network access. To prevent the user from remaining connected to the provisioning SSID, an access list that provides access only to ISE, DHCP, and DNS must be enforced on the provisioning SSID. The details of this SSID are discussed in the Client Provisioning section.

Table 9-3 shows the WLAN parameters for the SSIDs used in this design guide.

Table 9-3 WLAN Parameters

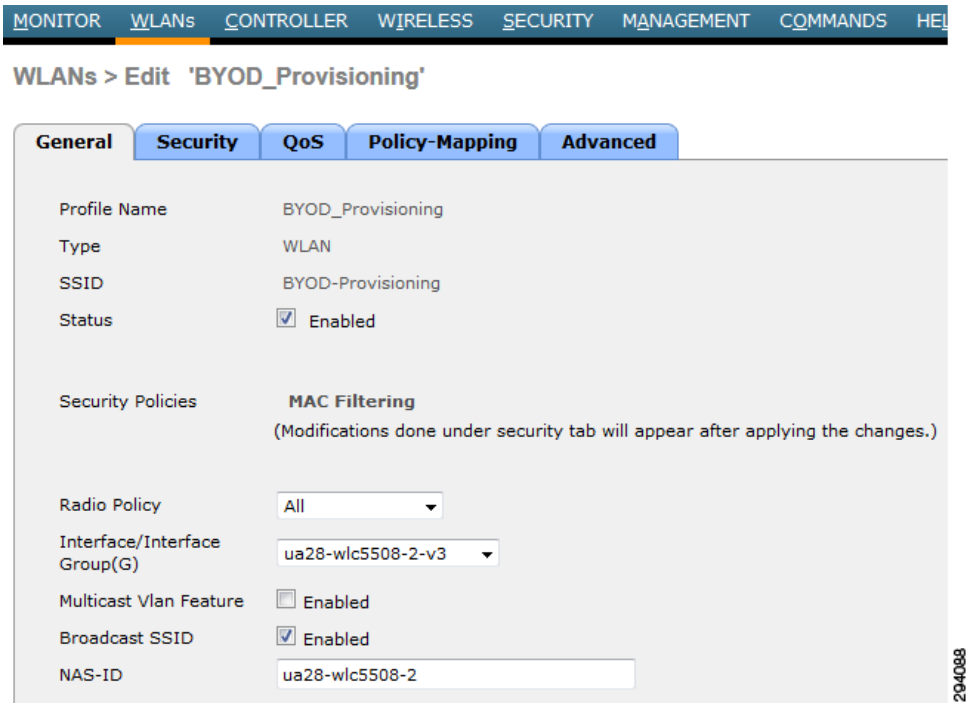
Attribute	BYOD_Provisioning	BYOD_Employee
Description	Used for device provisioning	For employees that have completed the on-boarding process
Layer 2 Security	None (for Open SSID)	WPA+WPA2
MAC Filtering	Enabled (for Open SSID)	Disabled
WPA+WPA2 Parameters	None (for Open SSID)	WPA2 Policy, AES, 802.1X
Layer 3 Security	None	None
AAA Server	Select ISE	Select ISE
Advanced	AAA Override Enabled	AAA Override Enabled
Advanced	NAC State-RADIUS NAC	NAC State-RADIUS NAC
Advanced-FlexConnect Local Switching	Disabled for Central Switching Provisioning Enabled for Local Switching Provisioning	Enabled

Table 9-3 WLAN Parameters

Attribute	BYOD_Provisioning	BYOD_Employee
Quality of Service	Best Effort	Platinum
AVC	Does Not Apply	Does Not Apply

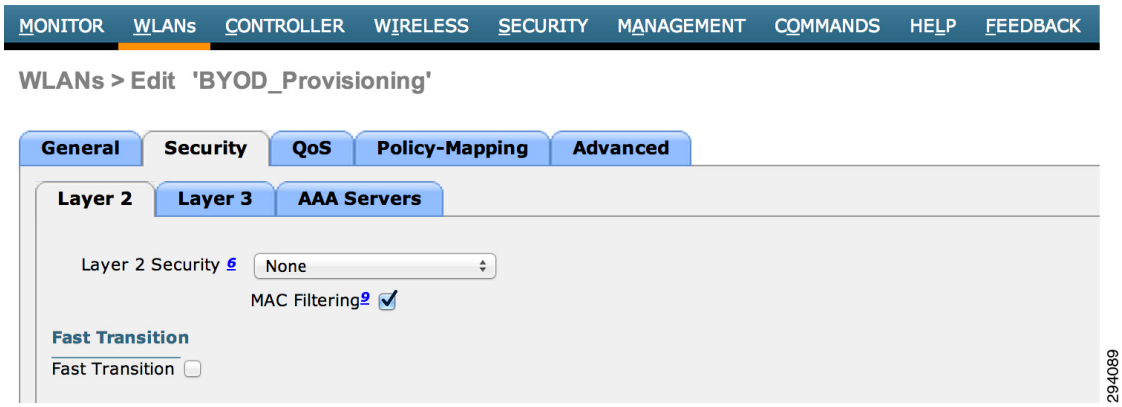
To create a WLAN, click **WLANs > Create New > Go** and provide the SSID and profile details. Figure 9-13 shows the general configuration details of the BYOD_Provisioning SSID.

Figure 9-13 Creating the Branch BYOD_Provisioning SSID



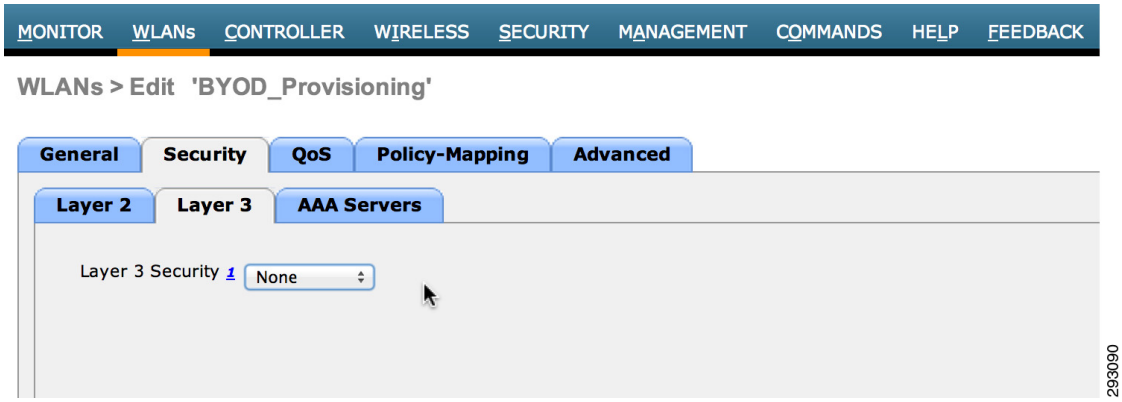
Since BYOD_Provisioning is an open SSID, the Layer 2 security settings in are configured as **None**. If the provisioning SSID had to be password-protected, the Layer 2 security settings would be configured as WPA+WPA2 Enterprise.

Figure 9-14 Layer 2 Security Settings



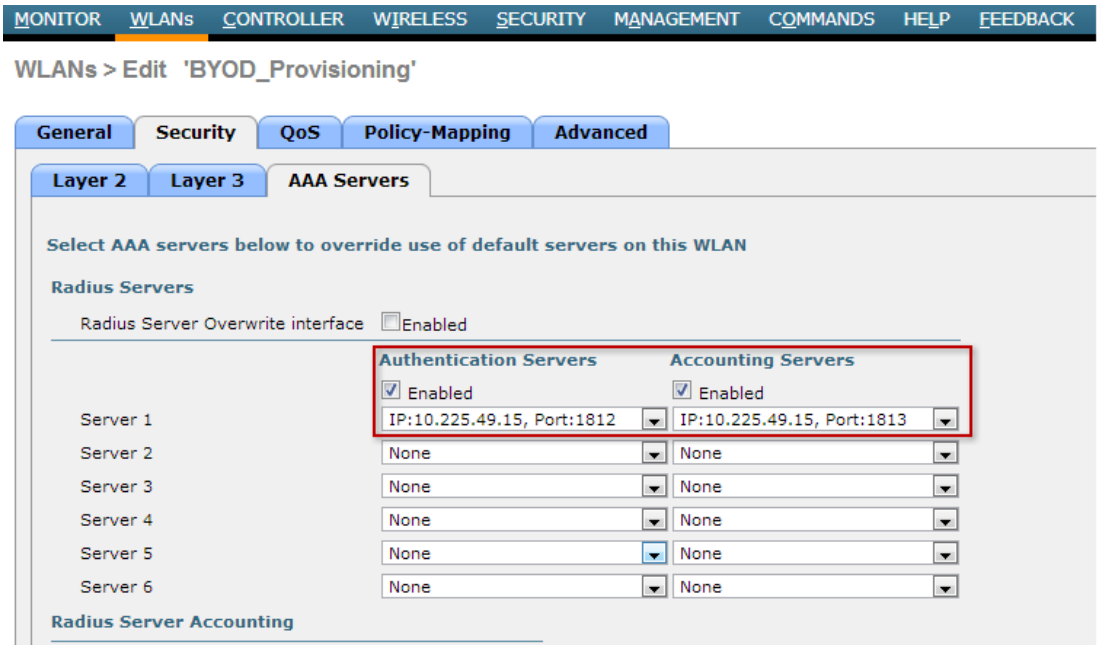
The Layer 3 Security is configured as **None**, as shown in Figure 9-15.

Figure 9-15 Layer 3 Security Settings



Under **Security > AAA servers**, configure the RADIUS server details. Figure 9-16 shows the ISE's IP address configured for Authentication and Authorization.

Figure 9-16 AAA Security Settings



Within the dual SSID deployment there are two possible ways to direct provisioning traffic:

- From the campus or data center—The endpoint receives an IP address from a DHCP scope at the data center and the provisioning traffic is directed through the CAPWAP tunnel between the branch and the Flex 7500 controller.
- At the branch—The endpoint receives an IP address from a DHCP scope at the branch and the provisioning traffic uses the switching and WAN infrastructure for connectivity to data center resources.

Dual SSID—Central Switching Provisioning

Figure 9-17 shows how with central switching provisioning, the endpoint communicates with ISE and data center resources using the CAPWAP tunnel and all traffic is tunneled back to the controller in the data center.

Figure 9-17 Central Switching Provisioning

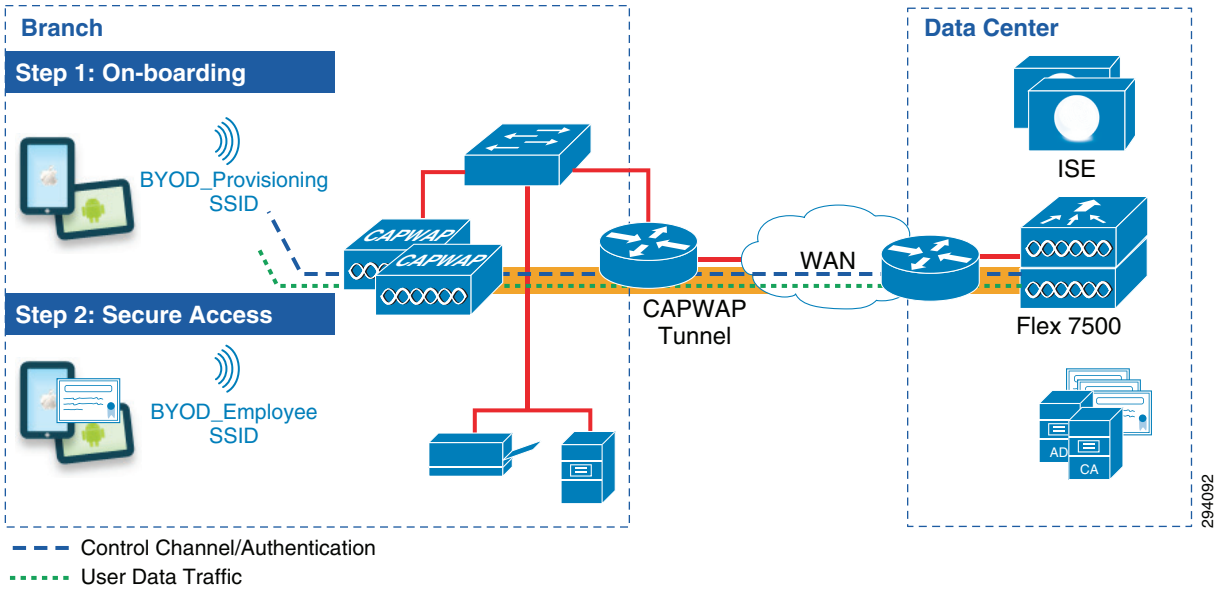
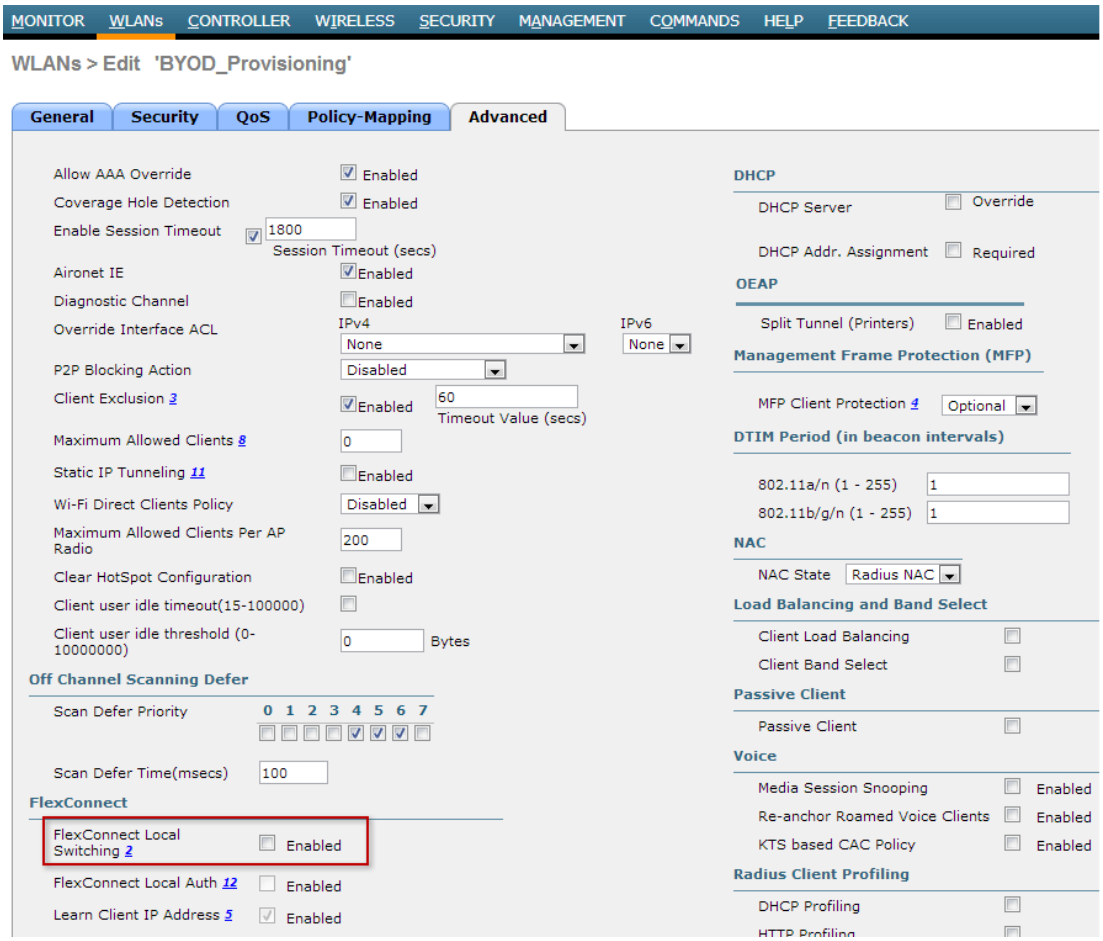


Figure 9-18 shows the advanced settings for BYOD_Provisioning, including the AAA Override and NAC State. The FlexConnect Local Switching setting is disabled for central switching provisioning.

Figure 9-18 Advanced Settings for Central Switching Provisioning



Note Authorization Policies and Profiles in Chapter 10, "Identity Services Engine for BYOD" shows the ACLs and authorization profiles used for dual and single SSID provisioning.

Dual SSID—Local Switching Provisioning

Figure 9-19 shows provisioning with local switching mode. The user data traffic is sent to the switch interface and the endpoint relies on the normal router/WAN infrastructure to reach the ISE and other network resources.

Figure 9-19 Local Switching Provisioning

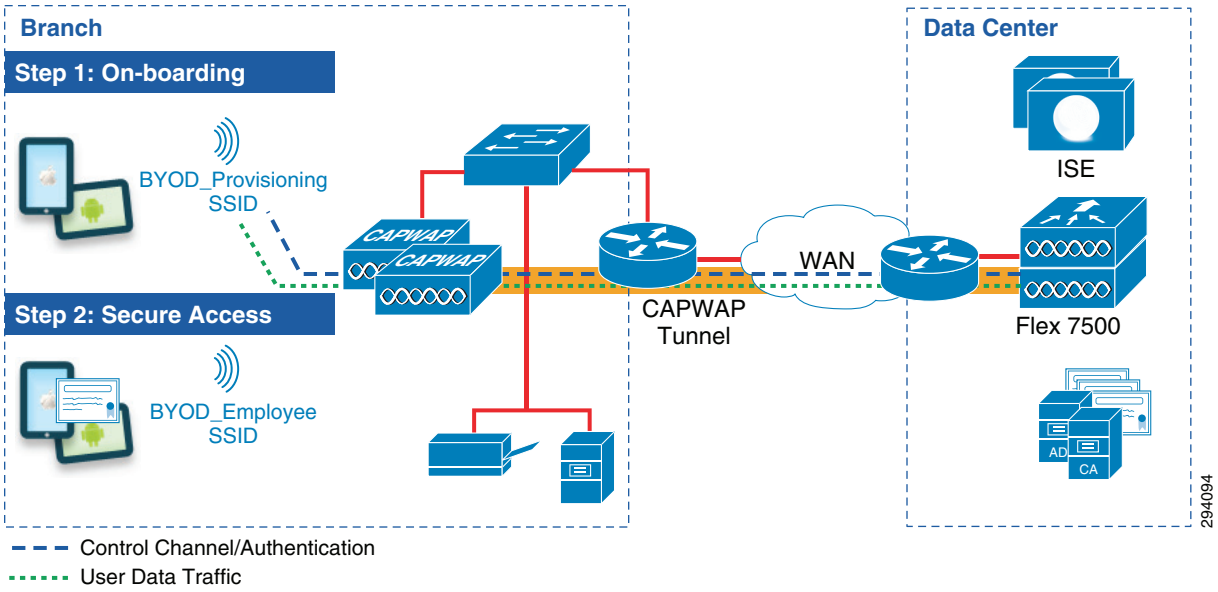
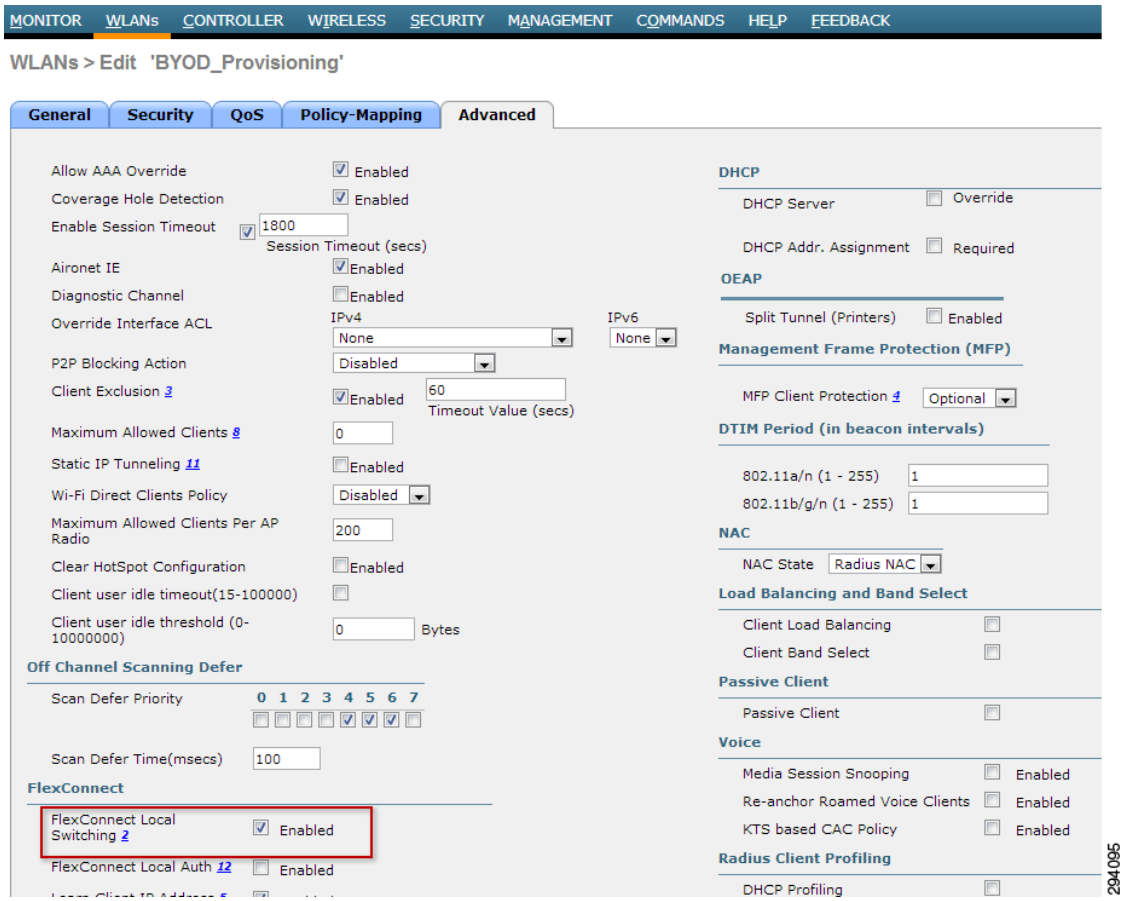


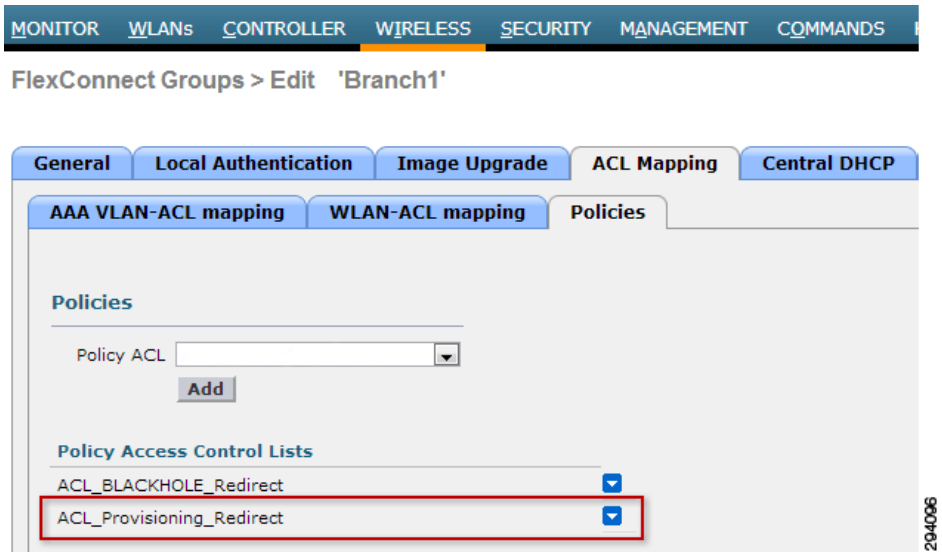
Figure 9-20 shows the advanced settings for BYOD_Provisioning, including the AAA Override and NAC State. The FlexConnect Local Switching is enabled for local switching provisioning.

Figure 9-20 Advanced Settings for Local Switching Provisioning



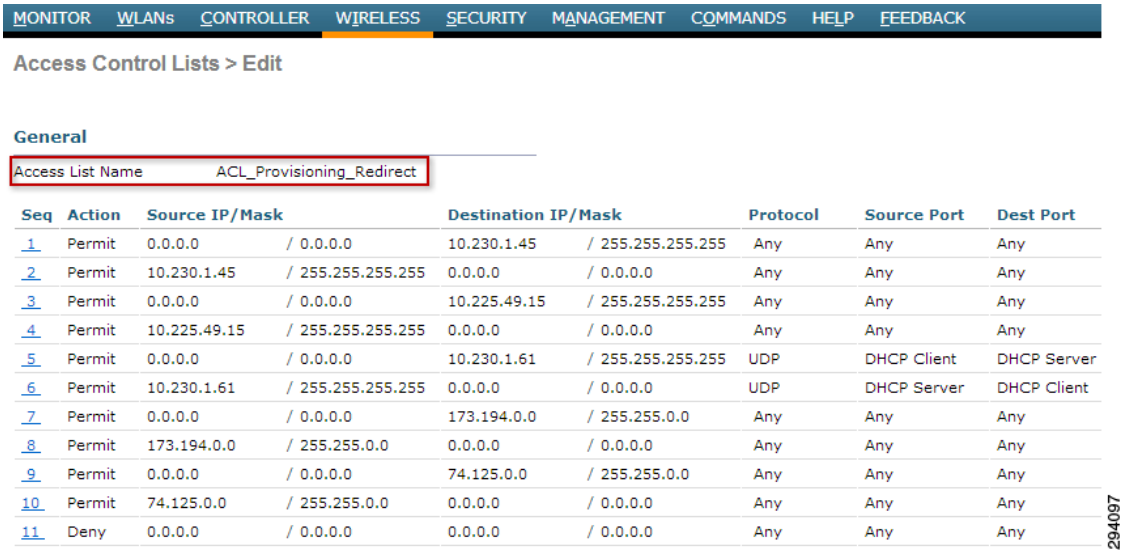
To enforce the redirection to the self-registration portal, a FlexConnect ACL is defined under the Policies tab for the specific FlexConnect group, as shown in Figure 9-21.

Figure 9-21 Policies for FlexConnect Group



The ACL_Provisioning_Redirect FlexConnect ACL shown in Figure 9-22 allows access to ISE, DNS, the Google Play Store, and denies all other traffic. Android devices require access to the Google Play Store to download the SPW package.

Figure 9-22 ACL_Provisioning_Redirect FlexConnect ACL



The ACL_Provisioning_Redirect ACL specifies the following access:

- Allow IP access to and from the DNS server (10.230.1.45).
- Allow IP access to and from the ISE Server (10.225.49.15).
- Allow IP access to and from the DHCP server (10.230.1.61).
- Access to Google Play.

Note The purpose of the ACL shown above is to provide an example that network administrators can use to deploy in the network. The Google and Apple app stores may change their addresses, so it is advisable to validate those addresses before deploying the ACL.

Note ACL_Provisioning_Redirect must redirect all traffic sent to enroll.cisco.com. The Cisco Configuration Assistant for Android devices requires this redirect to discover the IP address of the ISE server.

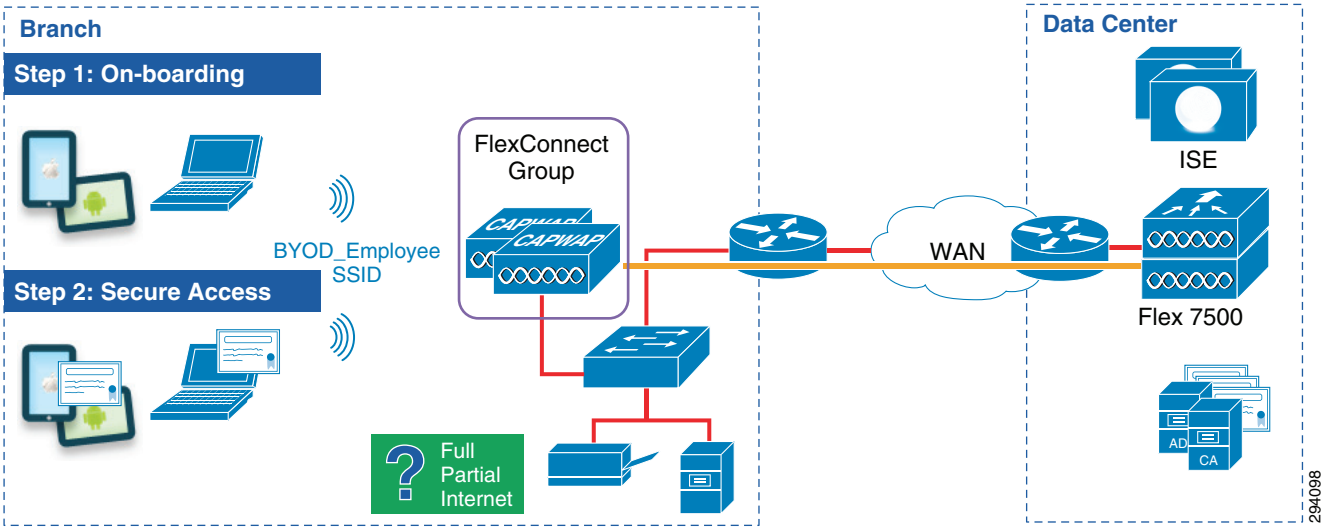
FlexConnect Branch—Single SSID Design

In a single SSID design, the same WLAN is used for certificate enrollment, provisioning (on-boarding process), and secure network access. There are some considerations that should be taken into consideration while deploying a Single SSID solution:

1. Since the authentication method is PEAP, the user is expected to enter the AD credentials before the registration process can begin. In the PEAP protocol, the server presents its identity certificate to the end user. In this design, ISE presents its identity certificate to the endpoint. Some endpoints may reject the certificate if the root certificate is not present in their list of trusted providers. During the registration process, the root CA certificate is installed on the endpoint, but this can't be done if the initial dialog itself fails. Hence, this presents a chicken-and-egg problem. To prevent this from happening the ISE identity certificate must be signed by a third-party trusted provider such as VeriSign.
2. If the above cannot be done, then it is better to deploy dual SSID design.

Figure 9-23 shows how this design uses the BYOD_Employee SSID and is implemented using the Flex 7500 Controller cluster, which is dedicated to manage the APs in the branch locations.

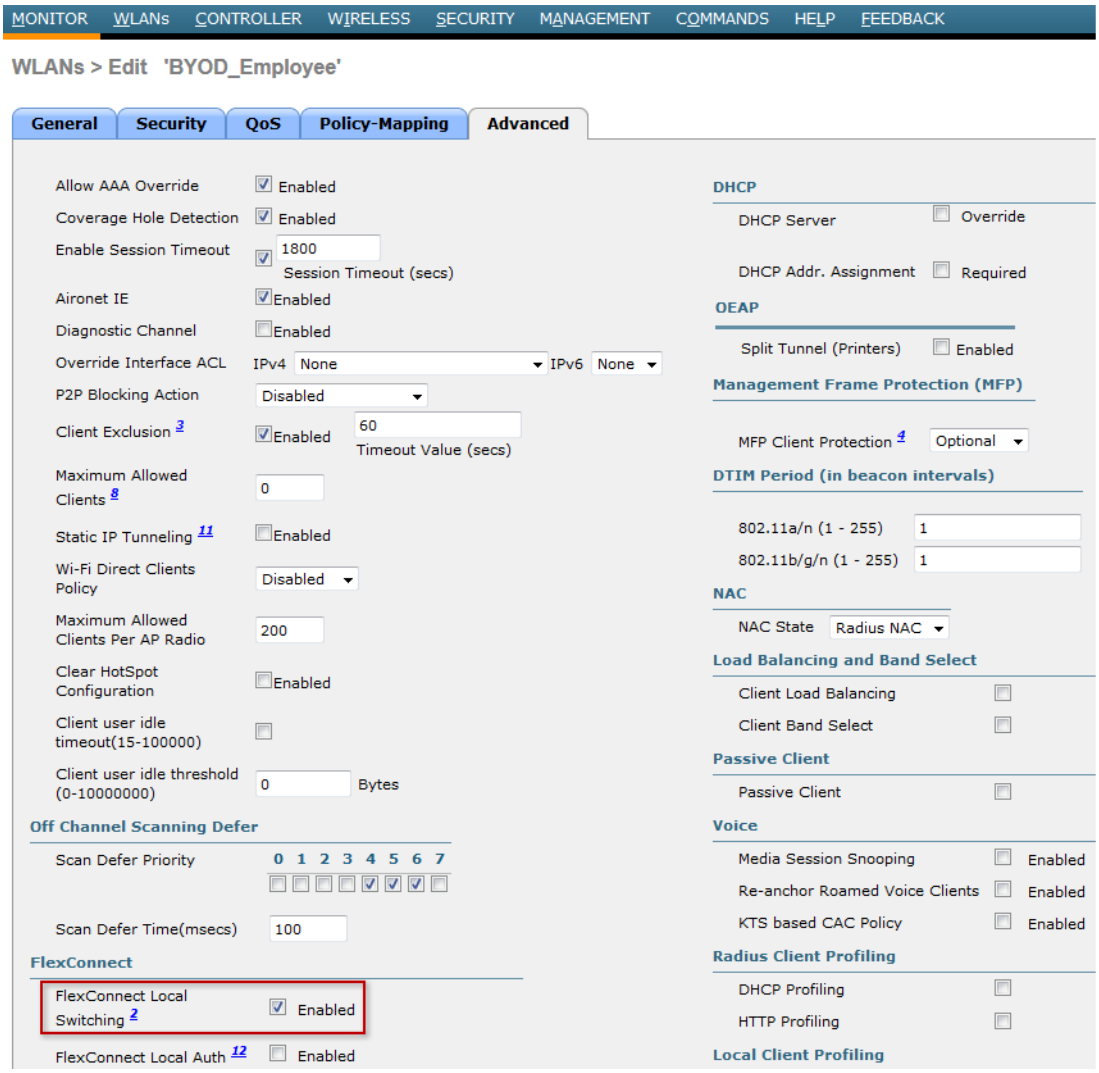
Figure 9-23 Branch-Single SSID



In this scenario the APs associate with the Flex 7500 controller and the FlexConnect capabilities allow the on-boarding and secure access capabilities to be handled by the single BYOD_Employee SSID.

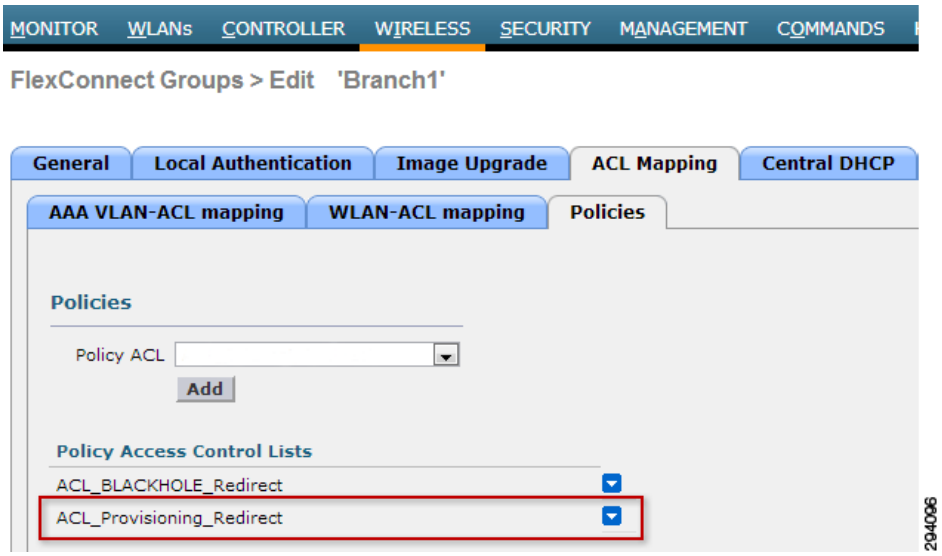
The steps to configure the BYOD_Employee WLAN are similar, following the parameters outlined in Table 9-3. It is important to note that FlexConnect Local Switching is enabled on the BYOD_Employee WLAN, as highlighted in Figure 9-24.

Figure 9-24 FlexConnect Local Switching



To enforce the redirection to the self-registration portal, a FlexConnect ACL is defined under the Policies tab, as shown in Figure 9-25.

Figure 9-25 Policies for FlexConnect Group



The ACL_Provisioning_Redirect ACL is shown in Figure 9-22 above.

FlexConnect Access Point Configuration

Configure the access point in FlexConnect mode by changing the AP Mode to FlexConnect. Click **Wireless > Access Points** and select the proper branch AP. Figure 9-26 shows the setting for an access point in Branch1.

Figure 9-26 FlexConnect AP Mode

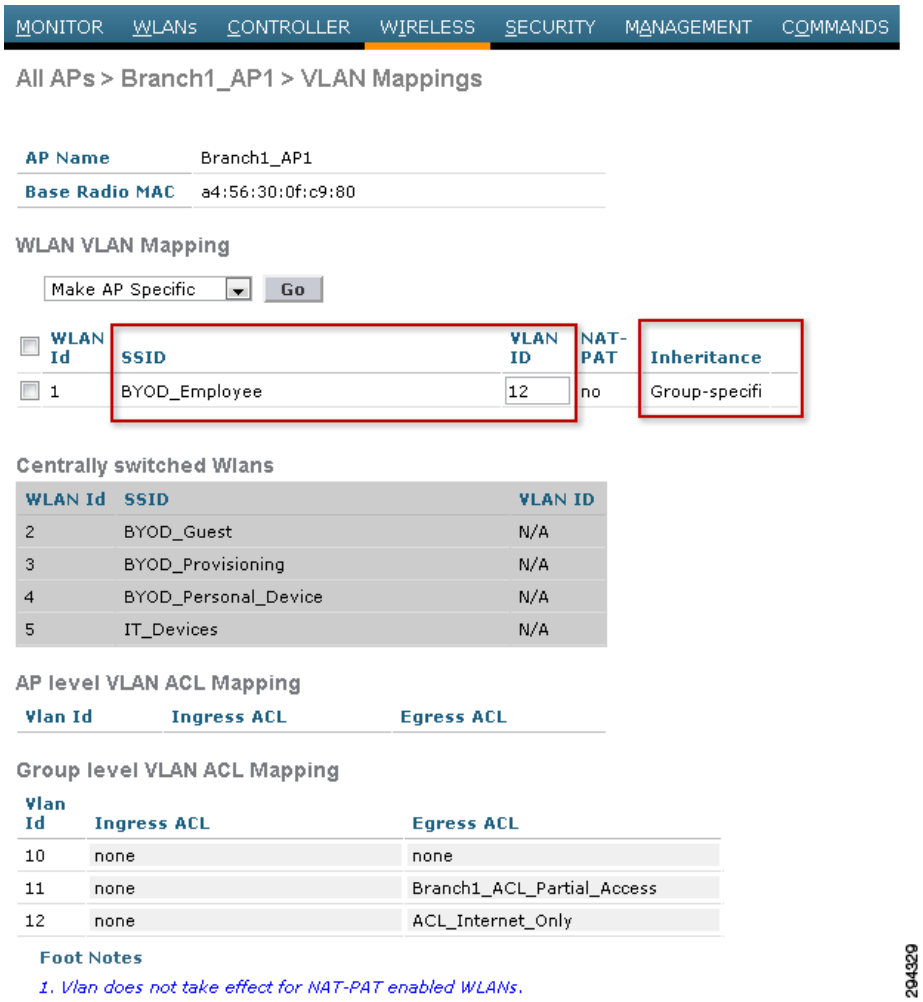
Click the **FlexConnect** tab and specify the Native VLAN for the branch, as shown in Figure 9-27. The access point relies on the native VLAN for IP connectivity.

Figure 9-27 Native VLAN ID

Define the VLAN ID to be used for local switching. In Figure 9-28, clients obtain an IP address from VLAN 12 (Internet access) when doing local switching. When using the AAA Overrides for FlexConnect feature, the client is moved to a different VLAN dynamically, based on the matched authorization profile and will obtain an IP address from the defined VLAN.

This setting can be configured at the AP level or the AP can inherit the settings from the FlexConnect Group. FlexConnect Groups are explained in the next section.

Figure 9-28 BYOD_Employee VLAN ID



FlexConnect Groups

FlexConnect groups provide a convenient way to group access points that share the same configuration settings. This is particularly helpful when grouping several FlexConnect access points in remote or branch locations. Instead of configuring each access point separately, FlexConnect groups allow the configuration parameters to be applied to all access points at once. For example, a FlexConnect ACL can be applied to a particular VLAN across all access points within a branch simply by adding the access points to the same FlexConnect group.

For the purpose of this guide, a unique FlexConnect group was defined for each branch, as shown in Figure 9-29.

Figure 9-29 FlexConnect Groups

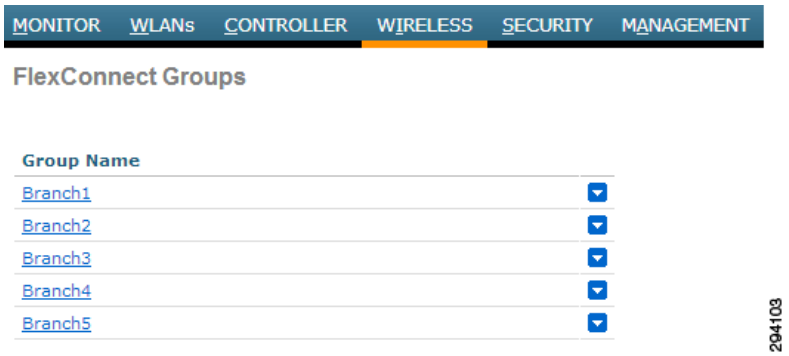
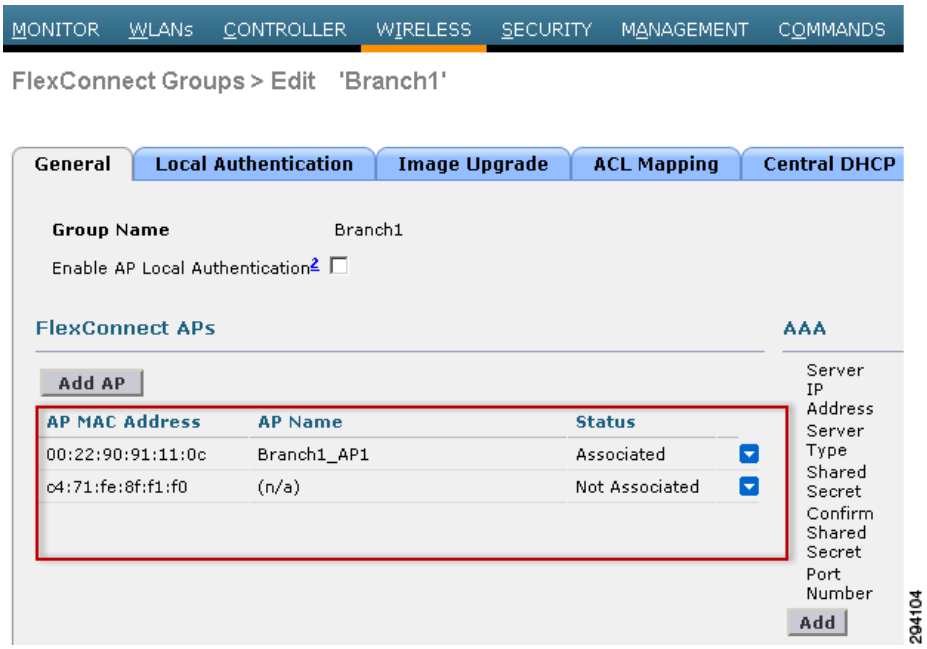


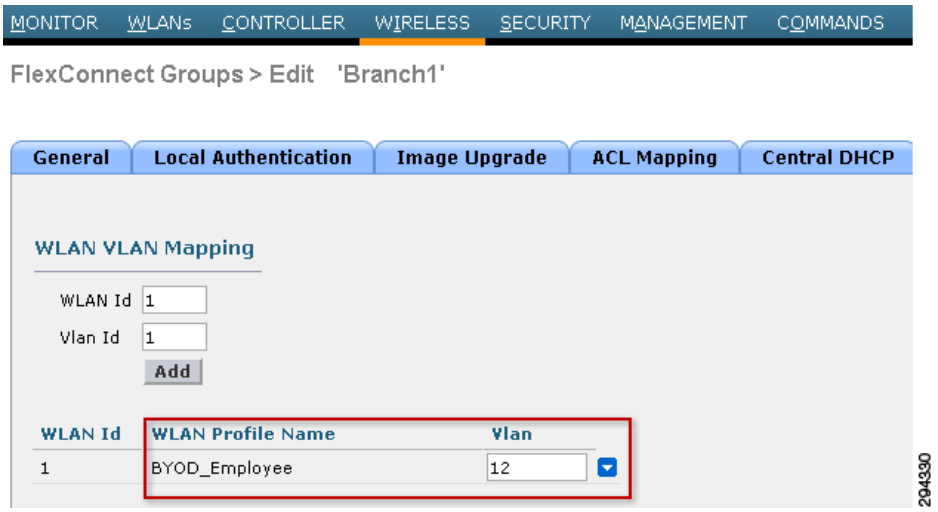
Figure 9-30 shows the access points that have been added to the Branch1 FlexConnect group.

Figure 9-30 Branch1 FlexConnect Group



The VLAN ID used for local switching can be defined at the AP level,as shown in Figure 9-28, or at the FlexConnect Group level, as shown in Figure 9-31. In this example, clients will obtain an IP address from VLAN 12 (Internet access) when doing local switching. When using the AAA Overrides for FlexConnect feature, the client is moved to a different VLAN dynamically based on the matched authorization profile and will obtain an IP address from the defined VLAN.

Figure 9-31 Local Switching VLAN—FlexConnect Group Level

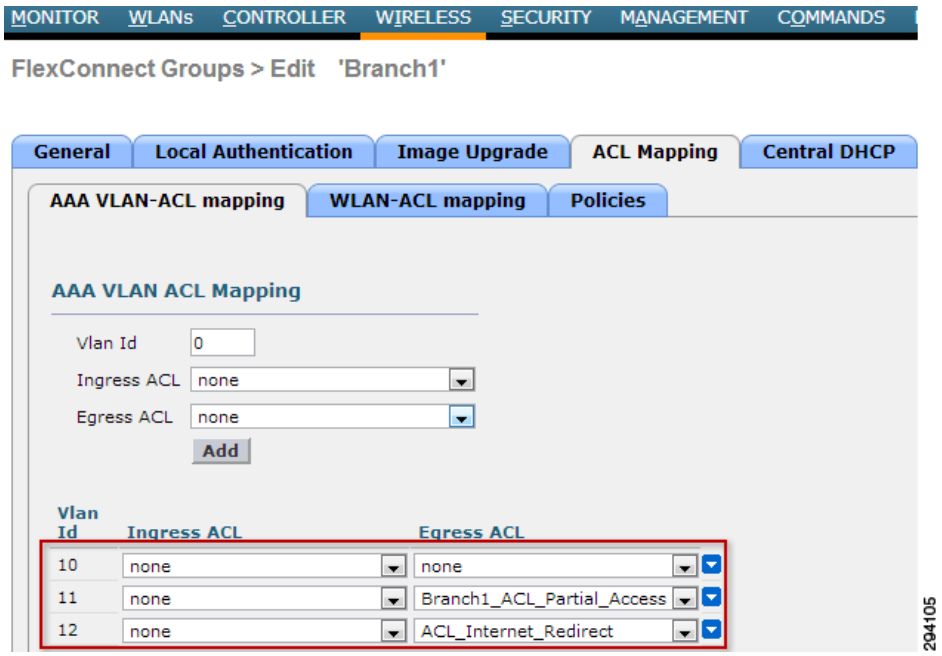


Before ISE can enforce an authorization policy, FlexConnect ACLs must be defined and assigned to each VLAN. By clicking the AAA VLAN-ACL mapping tab, the FlexConnect ACL may be enforced for each VLAN ID. This assumes that every branch location shares the same VLAN ID numbers:

- VLAN 10 for full access
- VLAN 11 for partial access
- VLAN 12 for Internet only access

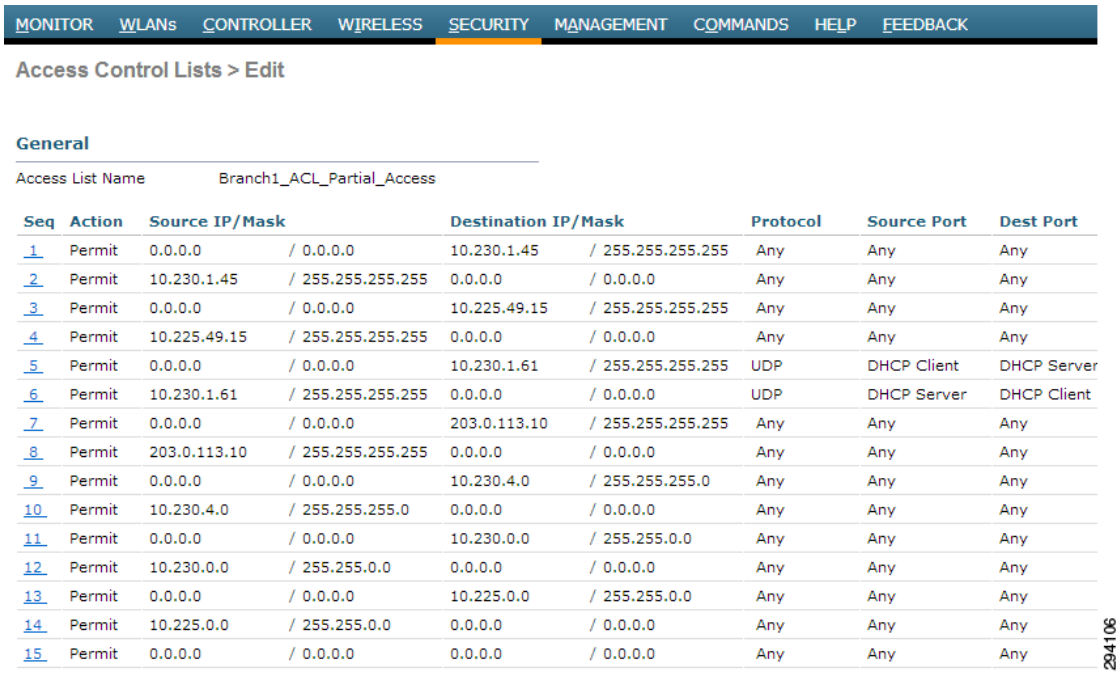
Figure 9-32 shows how the different FlexConnect ACLs have been mapped to each VLAN.

Figure 9-32 VLAN-ACL Mapping



The FlexConnect ACLs shown in Figure 9-33 and Figure 9-34 are explained in more detail in Chapter 15, "BYOD Enhanced Use Case—Personal and Corporate Devices."

Figure 9-33 Branch1_ACL_Partial_Access FlexConnect ACL



MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Access Control Lists > Edit

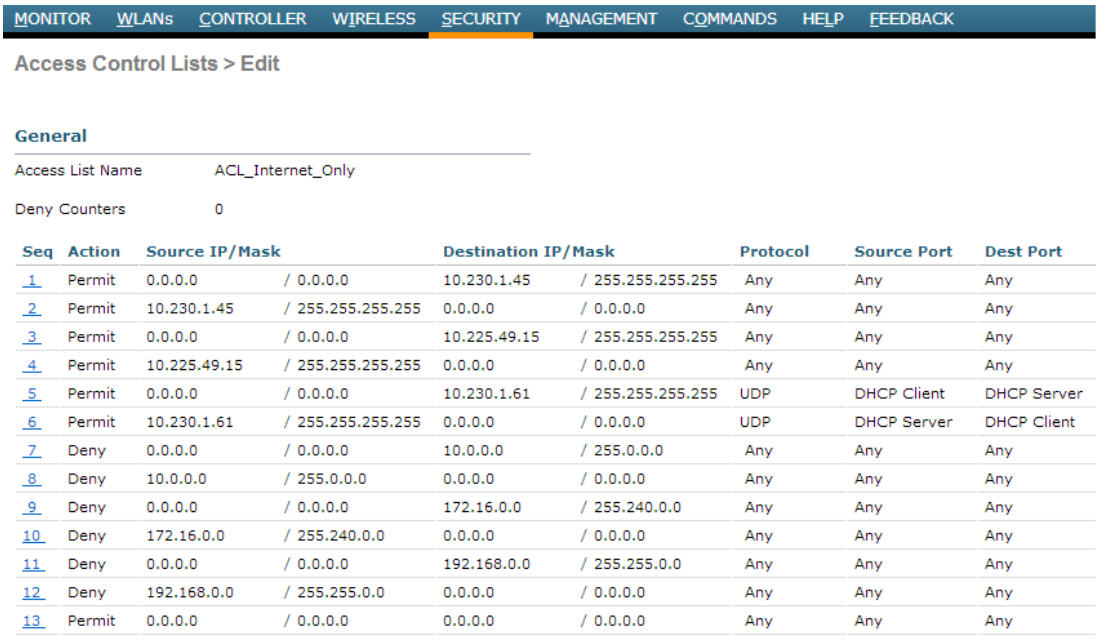
General

Access List Name Branch1_ACL_Partial_Access

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any
4	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server
6	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client
7	Permit	0.0.0.0	/ 0.0.0.0	203.0.113.10	/ 255.255.255.255	Any	Any	Any
8	Permit	203.0.113.10	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
9	Permit	0.0.0.0	/ 0.0.0.0	10.230.4.0	/ 255.255.255.0	Any	Any	Any
10	Permit	10.230.4.0	/ 255.255.255.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
11	Permit	0.0.0.0	/ 0.0.0.0	10.230.0.0	/ 255.255.0.0	Any	Any	Any
12	Permit	10.230.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
13	Permit	0.0.0.0	/ 0.0.0.0	10.225.0.0	/ 255.255.0.0	Any	Any	Any
14	Permit	10.225.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
15	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

294106

Figure 9-34 ACL_Internet_Only



MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Access Control Lists > Edit

General

Access List Name ACL_Internet_Only

Deny Counters 0

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any
4	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server
6	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client
7	Deny	0.0.0.0	/ 0.0.0.0	10.0.0.0	/ 255.0.0.0	Any	Any	Any
8	Deny	10.0.0.0	/ 255.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
9	Deny	0.0.0.0	/ 0.0.0.0	172.16.0.0	/ 255.240.0.0	Any	Any	Any
10	Deny	172.16.0.0	/ 255.240.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
11	Deny	0.0.0.0	/ 0.0.0.0	192.168.0.0	/ 255.255.0.0	Any	Any	Any
12	Deny	192.168.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
13	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

294107

FlexConnect VLAN Override

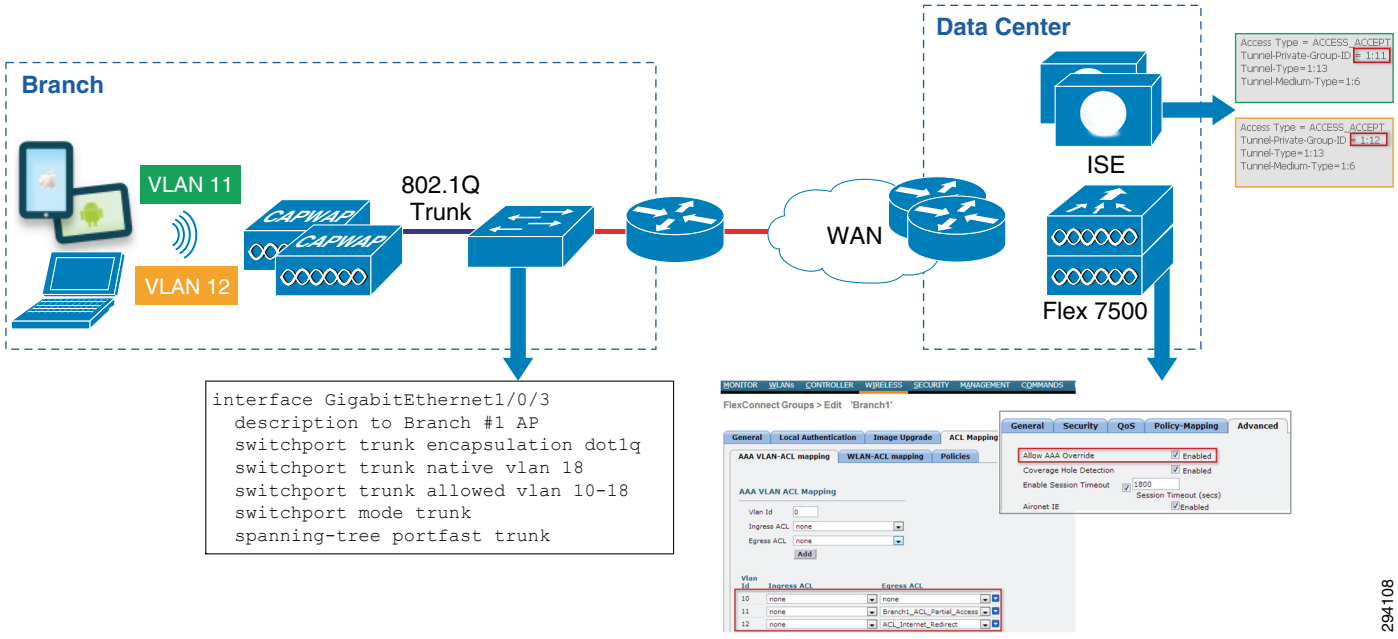
In the current FlexConnect architecture, there is a strict mapping of WLAN to VLAN, so the client getting associated on a particular WLAN on a FlexConnect AP has to abide by the VLAN which is mapped to it. This method has limitations because it requires clients to associate with different SSIDs in order to inherit different VLAN-based policies.

Starting on WLC release 7.2, AAA Override (Dynamic VLAN assignment) of VLANs on individual WLANs configured for local switching is supported. To assign endpoints dynamically to a VLAN, the VLAN IDs are pre-created and the corresponding WLAN-VLAN Mapping on a FlexConnect group is configured, as shown in Figure 9-32.

Figure 9-35 shows the different configuration settings required to dynamically assign endpoints to a branch VLAN, which include:

- The WLAN at the branch configured for local switching mode.
- 802.1Q trunk between the Catalyst switch and the access point.
- A native VLAN and allowed VLANs for the trunk.
- The ISE authorization profile defines what VLAN is assigned to the endpoint.
- The WLAN is configured at the controller to allow AAA Override.
- The VLANs are pre-defined and the VLAN-ACL mapping is defined for the FlexConnect group.

Figure 9-35 FlexConnect VLAN Override



Campus—Converged Access Design

The converged large campus design looks at the hybrid large campus design model, as discussed in Campus Migration Path of Chapter 5, "Campus and Branch Network Design for BYOD." A hybrid large campus design consists of multiple Catalyst 3850s switches or switch stacks deployed at the access layer

of the network, operating in Mobility Agent (MA) Mode. A centralized Cisco CT5760 controller within the campus contains the Mobility Controller (MC) function. A Unified Controller CT5508 exists within the campus controller and forms a mobility group with CT5760s. APs may be connected to the CT5760 or CT5508 controllers via Catalyst 3850 or CT3750 switches. In addition a CT5760 or CT5508 may be used as guest access anchor at the Internet edge of the campus. In this design guide the CT5508 is configured as a guest controller.

This design guide will make the following assumptions for the large campus converged access design:

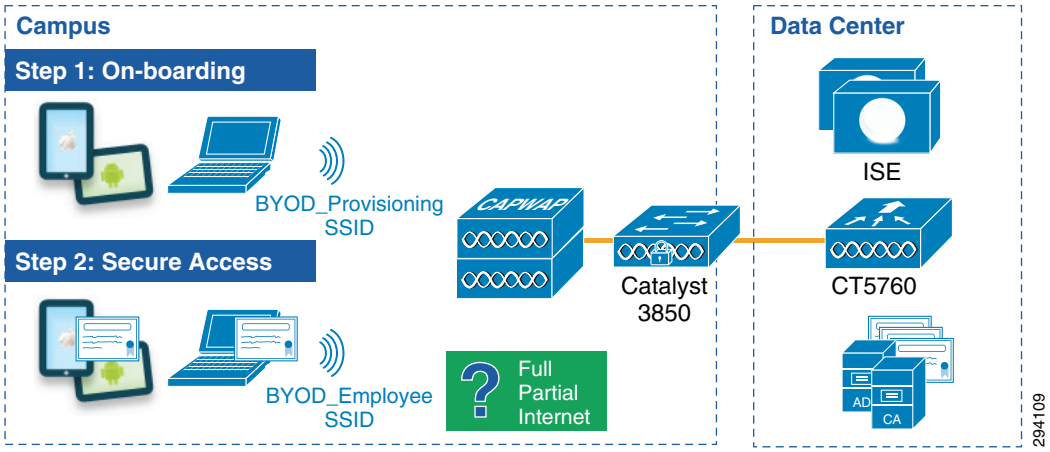
- On-boarded wired and wireless devices will share the same VLAN, and hence the same IP subnet addressing space. It is recognized that customers may implement separate subnets for wired and wireless devices due to issues such as additional security compliance requirements for wireless devices. This is not addressed within this version of the design guidance.
- Catalyst 3850 Series switches are deployed as Layer 2 access switches within the campus. Layer 3 connectivity will be provided by the Catalyst 6500 building distribution switches. Also, in keeping with campus best practices, VLANs will be limited to a single wiring closet. In other words, VLANs will not extend between access-layer switches. Future design guidance may address Catalyst 3850 Series switches deployed as Layer 3 switches or address spanning VLANs across access-layer switches.

Campus Converged Access—Dual SSID Design

In this design there are again two SSIDs: one provides enrollment/provisioning and the other provides secure network access. After connecting to the BYOD_Provisioning SSID and completing the enrollment and provisioning steps, the user connects to the BYOD_Employee SSID, which provides network access over a secure EAP-TLS connection.

Figure 9-36 shows the dual SSID design for the campus APs.

Figure 9-36 Campus—Dual SSID



In the converged access dual SSID design, there are some additional considerations:

- The provisioning SSID can be either open or password protected. When the provisioning SSID is open, any user can connect to the SSID, whereas if it is password protected, then only users that have credentials, such as AD group membership, are allowed to connect to the SSID. In this design guide, the provisioning SSID is configured to be open and its only purpose is to provide on-boarding services.

- After the device is provisioned, it is assumed that the user will switch to the second SSID for regular network access. To prevent the user from staying connected to the provisioning SSID, an access list that provides only access to ISE, DHCP, and DNS must be enforced on the provisioning SSID. The details of the ACL_Provisioning_Redirect ACL are shown below.
- This design guide makes use of the following SSIDs: BYOD_Provisioning and BYOD_Employee.

The properties of these two SSIDs are highlighted in Table 9-4.

Table 9-4 WLAN Parameters

Attribute	BYOD_Provisioning	BYOD_Employee
Description	Used only for device provisioning	For employees that have completed the on-boarding process
Layer 2 Security	None (for Open SSID)	WPA+WPA2
MAC Filtering	Enabled (for Open SSID)	Disabled
WPA+WPA2 Parameters	None	WPA2 Policy, AES, 802.1X
Layer 3 Security	None	None
AAA Server	Select ISE	Select ISE
Advanced	AAA Override Enabled	AAA Override Enabled
Advanced	NAC State- NAC	NAC State- NAC

To configure WLAN BYOD_Provisioning SSID on a CT5760 and Catalyst 3850 follow the steps below. The security on the BYOD_Provisioning SSID is NONE as this is a provisioning SSID through which devices are provisioned on the network. The FAST-SSID feature provides a way for a client to directly switch from BYOD_Provisioning to BYOD_Employee SSID after it has been properly provisioned by ISE.

```
aaa new-model
!
!
aaa authentication login default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
!
!
!
aaa server radius dynamic-author
 client 10.225.49.15 server-key 7 032A4802120A701E1D5D4C
!
aaa session-id common
!
ip device tracking
!
!
qos wireless-default-untrust
captive-portal-bypass
!
mac access-list extended MAC_ALLOW
 permit any any
!
!
interface Vlan2
 description ### BYOD-Employee Vlan ###
```

```
 ip address 10.231.2.7 255.255.255.0
 load-interval 30
!
interface Vlan3
 description ### BYOD-Provisioning Vlan ###
 ip address 10.231.3.7 255.255.255.0
 load-interval 30
!
ip http server
ip http authentication local
ip http secure-server
!
wireless management interface Vlan47
wireless client fast-ssid-change
wireless rf-network byod
wireless security dot1x radius call-station-id macaddress
wlan BYOD_Employee 1 BYOD_Employee
 aaa-override
 client vlan BYOD-Employee
 nac
 security web-auth parameter-map global
 session-timeout 1800
 no shutdown
wlan BYOD_Provisioning 3 BYOD_Provisioning
 aaa-override
 client vlan BYOD-Provisioning
 mac-filtering MAC_ALLOW
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 session-timeout 1800
 no shutdown
```

The example configuration shown above must be configured on both the Catalyst 3850 which functions as the Mobility Agent (MA), and the CT5760 which functions as the Mobility Controller (MC) in the campus design. Note that the IP addressing for the VLAN interfaces will be different for the MA and MC, however, since they are deployed in different parts of the network infrastructure. Mobility is handled as a separate topic within this chapter, following the WLAN configuration discussion. Additional configuration lines must be added to the MA and MC, respectively for mobility. These are discussed shortly.

The BYOD_Provisioning SSID has no Layer 2 security, as this is an SSID through which devices are provisioned on the network. Instead the wireless client uses MAC-filtering (basically a wireless version of MAB) to authenticate to the network. A URL re-direction and Centralized Web Authentication (CWA) policy is pushed down to the client from ISE, upon connecting to the network. Hence, the configuration for MAC-filtering, NAC, and AAA override are required on the BYOD_Provisioning SSID.

The security on the BYOD_Employee SSID is WPA2 with AES encryption. Note that this is the default setting for a WLAN on the Converged Access platforms (CT5760 or Catalyst 3850) and therefore does not appear within the configuration. The configuration for NAC and AAA override are required on this SSID in order to support a dynamic ACL assignment to the wireless client. In the case of this design guide, the dynamic ACL is a named ACL configured locally on the Catalyst 3850 switch.

Note The administrative level command **show wlan name *<name_of_wlan>*** can be used to show the details regarding the configuration of any WLAN on either the Catalyst 3850 Series switch or the CT5760 wireless controller. This includes any default settings which do not appear within the configuration.

Even though a CWA policy is pushed to the wireless client from ISE during on-boarding via the BYOD_Provisioning SSID, the HTTP and HTTPS server functionality must be globally enabled on the Catalyst 3850 Series switch. This is in order to support the URL re-direction of web sessions from wireless clients to the ISE provisioning portal. The RADIUS server group configuration points back to ISE as the RADIUS server for authentication and authorization of wireless (and wired) clients. The captive portal bypass functionality must be globally enabled on the Catalyst 3850 Series switch in order to allow Apple devices to on-board successfully. The fast-ssid-change global configuration provides a way for client to switch from BYOD_Provisioning to BYOD_Employee SSID after it has been properly provisioned by ISE.

The wireless mobility configuration commands for the CT5760 which functions as the MC will be different from the Catalyst 3850 which functions as the MA. An example of the global mobility configuration lines for the CT5760 wireless controller is shown below.

```
!
interface Vlan47
 description MGMT VLAN
 ip address 10.225.47.2 255.255.255.0
 load-interval 30
!
wireless mobility controller peer-group 100
wireless mobility controller peer-group 100 member ip 10.203.61.5 public-ip 10.203.61.5
wireless mobility controller peer-group 200
wireless mobility controller peer-group 200 member ip 10.207.61.5 public-ip 10.207.61.5
wireless mobility controller peer-group 200 member ip 10.207.71.5 public-ip 10.207.71.5
wireless mobility group member ip 10.225.50.36 public-ip 10.225.50.36/Points to CT5508
wireless mobility group name byod
wireless management interface Vlan47
wireless rf-network byod
!
```

As can be seen, the CT5760 is configured as the mobility controller (MC) for two switch peer-groups (SPGs)—100 and 200—in the example above. Switch peer-group 100 contains a single Catalyst 3850 switch functioning as a MA. Switch peer-group 200 contains two Catalyst 3850 switches functioning as MAs. An example of the global mobility configuration lines for the Catalyst 3850 is shown below.

```
interface Vlan47
 description MGMT VLAN
 ip address 10.225.61.5 255.255.255.0
 load-interval 30
!

wireless mobility controller ip 10.225.47.2 public-ip 10.225.47.2 / IP Address of 5760 MC
```

The IP address corresponding to the wireless management interface of the Catalyst 3850 series switch shown in the configuration above appears as a member of SPG 200. SPGs are designed to scale mobility within a Converged Access design. Roaming between Catalyst 3850 Series switch mobility agents (MAs) within a single SPG is handled directly by the switches without the involvement of the CT5760 mobility controller (MC). This is done via a full mesh of CAPWAP tunnels between the Catalyst 3850 Series switch mobility agents (MAs) within a single SPG. Roaming between Catalyst 3850 Series switch mobility agents (MAs) across two SPGs is handled by the CT5760 mobility controller (MC). This is done via CAPWAP tunnels between each Catalyst 3850 Series switch mobility agent (MA) and the CT5760 mobility controller (MC).

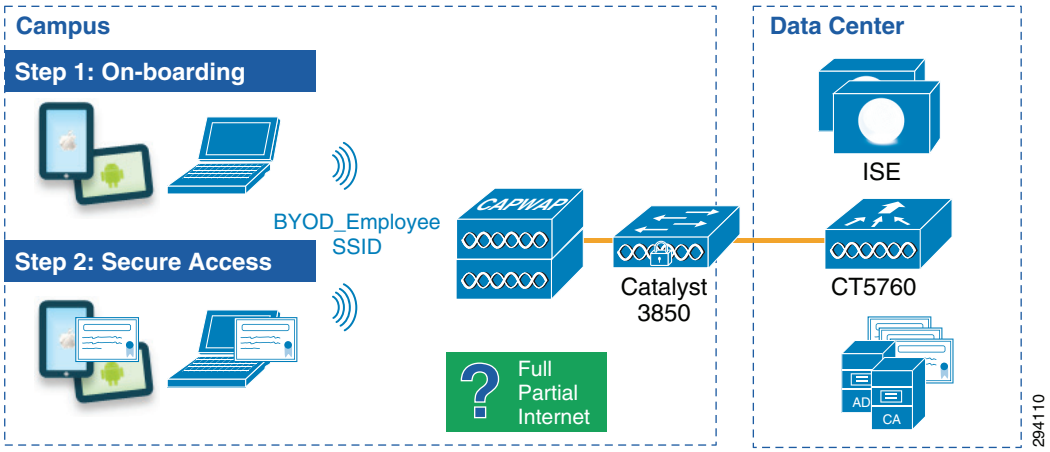
As discussed previously, a hybrid campus design may consist of CT5508 wireless controllers operating in Local Mode, alongside the Converged Access infrastructure. This may be necessary during the migration from a centralized wireless overlay model to a Converged Access deployment model. In order

to support mobility between the CT5508 wireless controller and the CT5760 wireless controller, the IP address of the CT5508 wireless controller has been added as a wireless mobility group member to the configuration of the CT5760 shown above.

Campus Converged Access—Single SSID Design

In a single SSID design the same WLAN (BYOD_Employee) is used for on-boarding and secure network access. Figure 9-37 shows how this design may be implemented using the CT5760 as an MC and Catalyst 3850 as MA.

Figure 9-37 Campus-Single SSID



The configuration for a single SSID converged campus design is almost the same as a dual SSID design but without the use of the BYOD_Provisioning SSID. A snippet of configuration on the CT5760 and the Catalyst 3850 is shown below. Mobility is handled as separate topic following the WLAN configuration discussion.

```
aaa new-model
!
!
aaa authentication login default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
!
!
!
aaa server radius dynamic-author
 client 10.225.49.15 server-key 7 032A4802120A701E1D5D4C
!
aaa session-id common
!
ip device tracking
!
!
qos wireless-default-untrust
captive-portal-bypass
!
mac access-list extended MAC_ALLOW
 permit any any
!
```

```
!
interface Vlan2
 description ### BYOD-Employee Vlan ###
 ip address 10.231.2.7 255.255.255.0
 load-interval 30
!
interface Vlan3
 description ### BYOD-Provisioning Vlan ###
 ip address 10.231.3.7 255.255.255.0
 load-interval 30
!
ip http server
ip http authentication local
ip http secure-server
!
wireless management interface Vlan47
wireless client fast-ssid-change
wireless rf-network byod
wireless security dot1x radius call-station-id macaddress
wlan BYOD_Employee 1 BYOD_Employee
 aaa-override
 client vlan BYOD-Employee
 nac
 security web-auth parameter-map global
 session-timeout 1800
 no shutdown
```

The mobility configuration for both the MC and MA will remain the same as discussed above for the dual SSID Converged Access design.

Campus Converged Access—Mobility

For the large campus design it is important to understand mobility and roaming considerations.

This design highlights multiple Catalyst 3850 Series switches or switch stacks deployed at the access layer of a large sized campus. Switch stacks form Switch Peer Groups (SPGs) in which all switches contain the Mobility Agent (MA) function. Roaming within a SPG is handled through a full mesh of mobility tunnels between MAs within the SPG. Multiple SPGs exist within the large sized campus. APs must be directly connected to MA and not via an intermediate switch (example: a Catalyst 3750 switch).

A Cisco CT5760 wireless controller deployed within a centralized service module within the campus contains the Mobility Controller (MC) function. Multiple SPGs connecting to a single MC form a Mobility Sub-Domain. Multiple Mobility Sub-Domains exist within the large sized campus. Roaming between SPGs within a Mobility Sub-Domain is done through the Cisco CT5760 and/or CT5508 wireless controller. APs connected to a Catalyst 3850 switch register with the CT5760 MC. APs can also be connected to CT5760 via Catalyst 3750 switches.

Multiple Cisco CT5760 and/or CT5508 wireless controllers form a Mobility Group. Hence, a Mobility Group also consists of multiple Mobility Sub-Domains. Roaming between Mobility Sub-domains is done through the Cisco CT5760 and/or CT5508 wireless controllers within the Mobility Group. A single Mobility Group and hence a single Mobility Domain extends across and are entirely contained within the large campus within this design.

For hybrid models consisting of both a CUWN local-mode and converged access products, either a Cisco CT5760 or a CT5508 also serves as a wireless controllers for access points connected to Catalyst 3750-X Series switches using traditional local mode (centralized switching) wireless connectivity.

Keeping above the considerations in mind, few things should be kept in mind.

By default Catalyst 3850 operates as a Mobility Agent and there is no need of any configuration. A Catalyst 3850 may also operate as a Mobility Controller. This mode is covered as part of Branch Design.

See Appendix C, "Software Versions" for details about the Catalyst 3850 software licensing.

CT5760 wireless controller operates only as a Mobility Controller. Mobility tunnels should be setup between CT5760s and Catalyst 3850s for APs connected on Catalyst 3850s to be registered with the MC (CT5760). A snippet of configuration for MC is as below:

```
wireless mobility controller peer-group 100
wireless mobility controller peer-group 100 member ip 10.203.61.5 public-ip 10.203.61.5
wireless mobility controller peer-group 200
wireless mobility controller peer-group 200 member ip 10.207.61.5 public-ip 10.207.61.5
wireless mobility controller peer-group 200 member ip 10.207.71.5 public-ip 10.207.71.5
```

On each Catalyst 3850 acting as an MA, the configuration below is needed to establish a mobility tunnel with the CT5760 MC or a 5508 MC.

```
wireless mobility controller ip 10.225.47.2 public-ip 10.225.47.2 / IP Address of MC
```

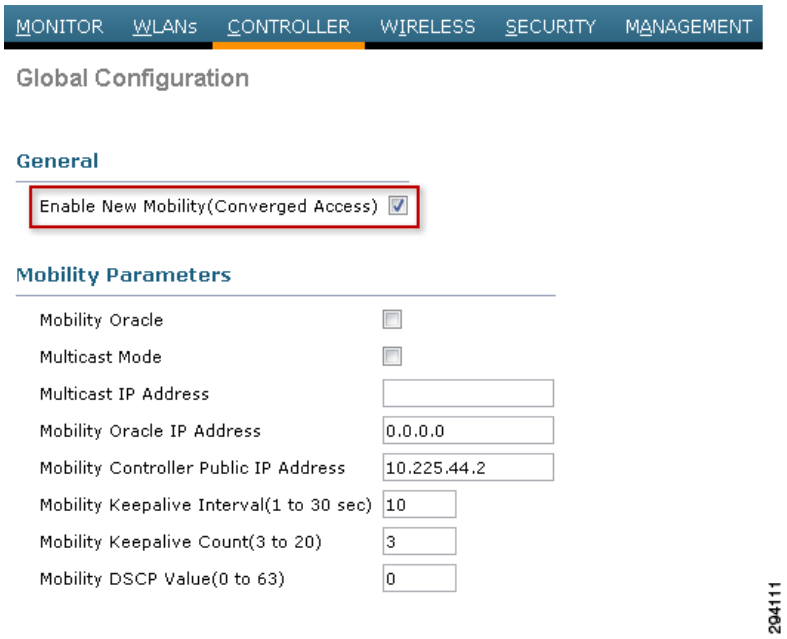
The CT5508 and CT5760 can also form a mobility group. The CT5508 should be upgraded to either 7.3.112 or a version above 7.5 of the WLC to support mobility between converged access and unified access products. The configuration on the CT5508 to enable mobility between the CT5760 and the CT5508 is shown below. The design guide provides guidance for version 7.5 for CT5508.

```
wireless mobility controller/ Enables the MC function, by default turned on CT5760
wireless mobility group name byod/ Create mobility group byod
wireless mobility group member ip 10.225.50.36 public-ip 10.225.50.36/ IP of member CT5508
```

Note Only WLC versions 7.3.112 or 7.5 and above support mobility between converged access products and unified access products. Ensure that you have code version running compatible code. This design guide uses 7.5 release.

To enable mobility between converged access and unified access products, first the New Mobility should be enabled on the WLC as shown in Figure 9-38.

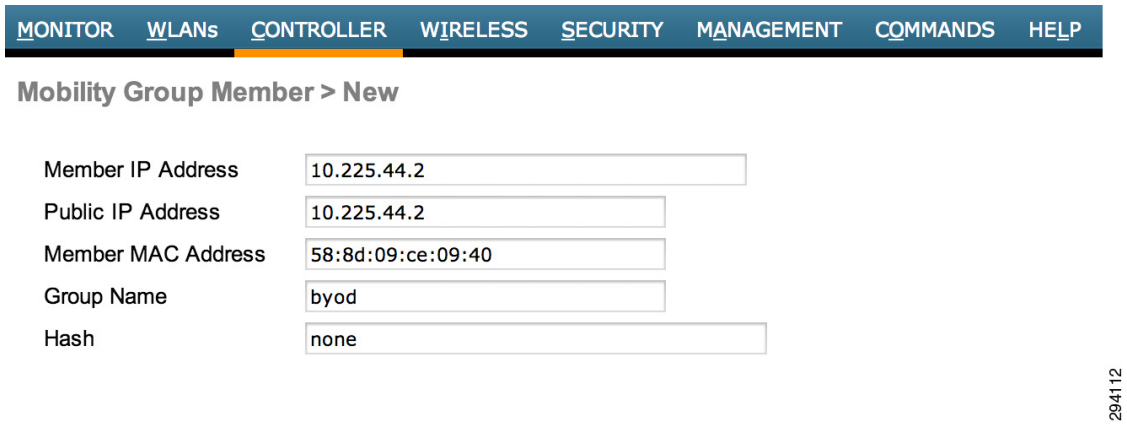
Figure 9-38 Enable New Mobility



After enabling New Mobility and restarting the Wireless LAN Controller, additional options for configuring switch peer groups as well as mobility groups are enabled. For CT5760 and CT5508 to form a group and talk to each other, additional configuration as below is required.

Click **Mobility Management > Mobility Groups** and click **New**, as shown in Figure 9-39.

Figure 9-39 Create New Mobility Group



The Member IP address above should be the CT5760 IP address that enables mobility messaging and CAPWAP tunnels to be set up between CT5760 and CT5508.

Other design considerations while deploying a large campus WLAN infrastructure include the following:

- 802.1X, WLAN, and VLAN configurations should be replicated on all Catalyst 3850s and CT5760s.
- Mobility group name should be the same between CT5760s and CT5508s.

Branch—Converged Access Design

With a converged access design, a centralized FlexConnect wireless controller can be replaced by a Catalyst 3850 switch that operates both as a Mobility Agent (MA) and Mobility Controller (MC). Guest wireless access still utilizes the same model wherein the guest traffic is auto-anchored to a dedicated guest anchor controller located within the Internet Edge of the campus. The guest controller can be a CT5508 controller with a 7.5 version of code, or a CT5760 converged wireless LAN controller.

The integrated controller branch BYOD design guide makes the following assumptions:

- On-boarded wired and wireless devices will share the same VLAN and hence the same IP subnet addressing space. It is possible to use different VLAN and addressing space for wireless and wired clients, however it is not addressed in this design guide.
- The Catalyst 3850 switches are deployed as a Layer 2 switches within the branch location. Layer 3 connectivity within the branch will be provided by ISR routers which also serve as the WAN connectivity point for the branch. (Future design guides may address Catalyst 3850 deployed as Layer 3 switch within the branch location).

Branch Converged Access—Dual SSID Design

In the dual-SSID design, a dedicated open SSID (BYOD_Provisioning) with MAC-filtering (i.e., MAC Authentication Bypass) will be configured for on-boarding devices. The SSID will be statically mapped to a separate Provisioning VLAN on the Catalyst 3850 switch. Figure 9-40 shows the branch converged access for a dual SSID design.

Figure 9-40 Branch Converged Access—Dual SSID

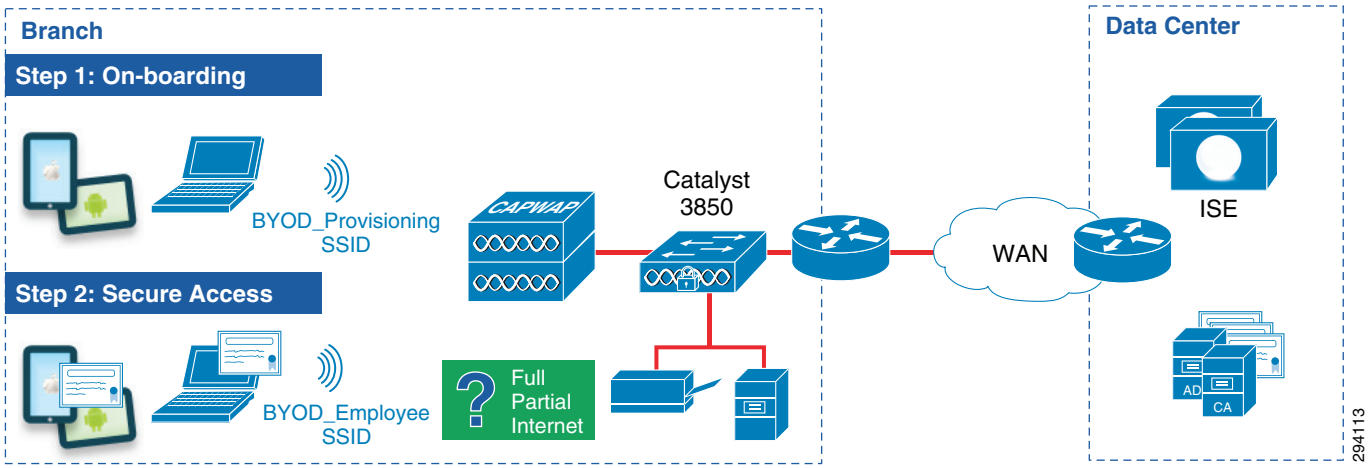


Table 9-5 summarizes the VLANs within the branch when utilizing the dual-SSID BYOD on-boarding design.

Table 9-5 VLANs in Branch with Dual-SSID BYOD On-boarding Design

Description	VLAN	VLAN Name
Wired and wireless corporate access. IT managed devices. Employee managed devices with full, partial, or Internet access.	12	BYOD_Employee
Provisioning VLAN for Dual-SSID wireless on-boarding.	13	BYOD_Provisioning
Separate VLAN for branch servers.	16	Server
Dedicated VLAN for management of network infrastructure.	18	Management
Isolated VLAN for pass through of wireless auto-anchor tunnels. Not trunked to Layer 3 router.	777	BYOD_Guest

The following configuration snippet provides an example of the possible configuration additions to the Catalyst 3850 in order to support on-boarding of wireless devices in a dual-SSID BYOD implementation using MAC-filtering.

```
aaa new-model
!
!
aaa authentication login default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
aaa server radius dynamic-author
 client 10.225.49.15 server-key 7 032A4802120A701E1D5D4C
 auth-type any
!
aaa session-id common
!
ip device tracking
!

qos wireless-default-untrust
vtp domain bn
!
mac access-list extended MAC_ALLOW
 permit any any
!
wireless mobility controller
wireless mobility group member ip 10.225.50.36 public-ip 10.225.50.36
wireless mobility group name byod
wireless management interface Vlan18
wireless client fast-ssid-change
wireless rf-network byod
wireless security dot1x radius call-station-id macaddress
wireless broadcast
wireless multicast
wlan BYOD_Employee 1 BYOD_Employee
 aaa-override
 client vlan BYOD_Employee
 nac
 security dot1x authentication-list default
 session-timeout 1800
 no shutdown
wlan BYOD_Guest 2 BYOD_Guest
 aaa-override
 client vlan BYOD_Guest
 mobility anchor 10.225.50.36
```

```
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 session-timeout 1800
 no shutdown
wlan BYOD_Provisioning 3 BYOD_Provisioning
 aaa-override
 client vlan BYOD_Provisioning
 mac-filtering MAC_ALLOW
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 session-timeout 1800
 no shutdown
!
```

The following configuration snippet provides a partial example of the possible configuration additions to the branch router configuration in order to support on-boarding of wireless devices in a dual-SSID BYOD implementation using MAC-filtering—when the Catalyst 3850 Series switch is functioning as a Layer 2 switch.

```
!
interface GigabitEthernet0/0
 description CONNECTION TO CATALYST 3850 SWITCH
 no ip address
 load-interval 30
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.13/ Provisioning VLAN
 description CATALYST 3850 PROVISIONING VLAN
 encapsulation dot1Q 13
 ip address 10.200.13.2 255.255.255.0
 ip helper-address 10.230.1.61/ Relay DHCP to the DHCP server
 ip helper-address 10.225.42.15/ Relay DHCP to ISE for profiling
 standby 13 ip 10.200.13.1
 standby 13 priority 110
 standby 13 preempt
!
```

Branch Converged Access—Single SSID Design

In the single SSID design, the corporate SSID (BYOD_Employee) supports authentication via PEAP for non on-boarded devices. Once on-boarding is complete, the corporate SSID supports authentication via EAP-TLS for on-boarded devices. The corporate SSID is statically mapped to a separate Corporate VLAN on the Catalyst 3850 switch. Figure 9-41 shows the branch converged access for a single SSID Design.

Figure 9-41 Branch Converged Access—Single SSID

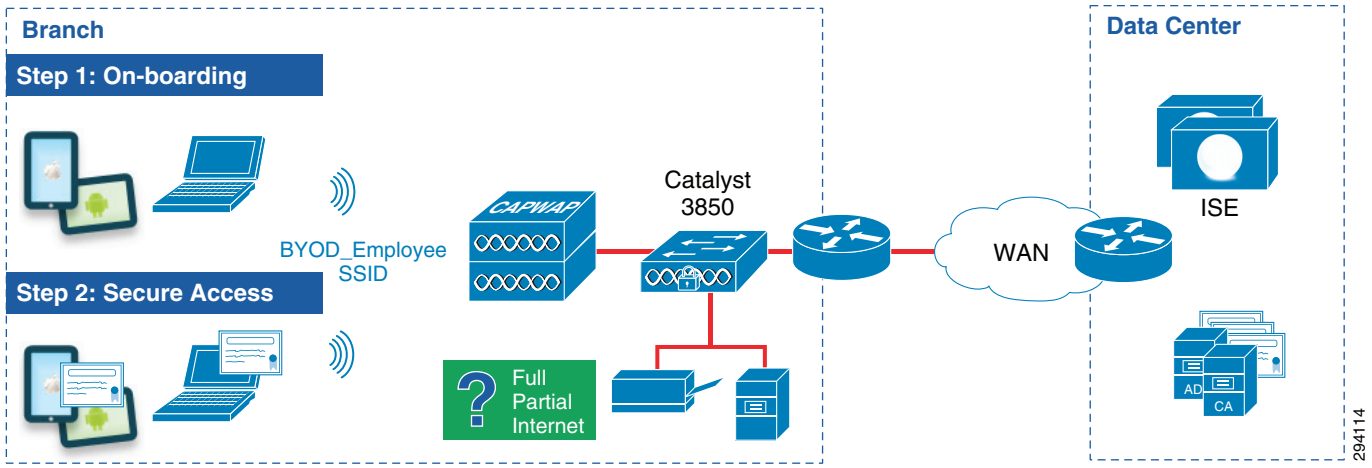


Table 9-6 summarizes the VLANs within the branch when utilizing the single-SSID BYOD on-boarding design.

Table 9-6 VLANs in Branch when Utilizing Single-SSID BYOD On-boarding Design

Description	VLAN	VLAN Name
Wired and wireless corporate access. IT managed devices. Employee managed devices with full, partial, or Internet access.	12	BYOD_Employee
Separate VLAN for branch servers.	16	Server
Dedicated VLAN for management of network infrastructure.	18	Management
Isolated VLAN for past through of wireless auto-anchor tunnels. Not trunked to Layer 3 router.	777	BYOD_Guest

The following configuration shows relevant parts of configuration for the Catalyst 3850 when utilizing a single SSID on-boarding model.

```
aaa new-model
!
!
aaa authentication login default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
aaa server radius dynamic-author
 client 10.225.49.15 server-key 7 032A4802120A701E1D5D4C
 auth-type any
!
aaa session-id common
!
ip device tracking
!
!
qos wireless-default-untrust
!
mac access-list extended MAC_ALLOW
 permit any any
!
```

```
wireless mobility controller
wireless mobility group member ip 10.225.50.36 public-ip 10.225.50.36
wireless mobility group name byod
wireless management interface Vlan18
wireless client fast-ssid-change
wireless rf-network byod
wireless security dot1x radius call-station-id macaddress
wireless broadcast
wireless multicast
wlan BYOD_Employee 1 BYOD_Employee
 aaa-override
 client vlan BYOD_Employee
 nac
 security dot1x authentication-list default
 session-timeout 1800
 no shutdown
wlan BYOD_Guest 2 BYOD_Guest
 aaa-override
 client vlan BYOD_Guest
 mobility anchor 10.225.50.36
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 session-timeout 1800
 no shutdown
!
?
```